1105 MEDIA

www.securitytoday.com

SECURITY today

Technology | Education | Solutions

September 2020 | Vol. 24 No. 6

Using AI Power

Driving efficiency and effectivity across organizations

NIGHTLOCK® LOCKDOWN ALERT

EMERGENCY MASS NOTIFICATION

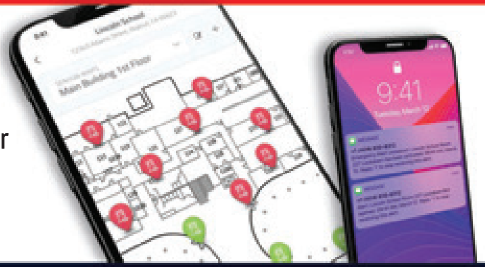
New NIGHTLOCK ALERT UPGRADE

- Installs with new Nightlock Lockdown devices or easily retrofits to your existing Nightlock door barricade system to add alert capabilities.
- Instantly Alerts: School Authorities, Teachers and Police Department when Wall Box is OPENED or Locking Handle is ENGAGED.
- Increases Police Response time.
- Panic Button System also available.

TAKE ACTION FASTER

FULL VISIBILITY FLOOR PLAN VIEW

Floor plan view to remotely monitor when and where barricades have been activated, in real-time.

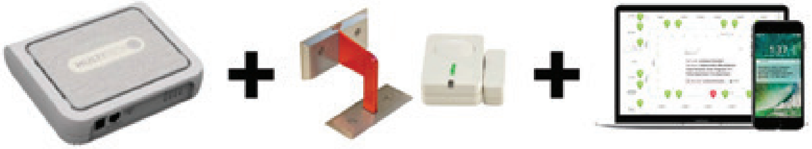


SMS TEXT ALERTS

Receive instant alerts when the barricade handle is accessed and when it is locked.

AUTOMATED SYSTEM = COMPLETE PROTECTION

Scan the devices. Add an unlimited number of alert recipients. Monitor door barricade status 24/7.



UNLIMITED ALERT RECIPIENTS

Automatically send instant alerts to teachers, administrators, emergency personnel, and more.

END-TO-END SECURITY

From the gateway to the sensors and alert system, Data is protected with AES 128-encryption.

LIFE TIME GUARANTEE

Should any sensor stop working, we'll replace it for free. 100% guaranteed.

THE NIGHTLOCK COMMITMENT

NIGHTLOCK®

Email: sales@nightlock.com
855.644.4856

THE
NEXT STEP
IN ACCESS
POWER

WINNER 2019
IoT
INTEGRATION
AWARDS
CEPro
Altronix

SECURITY today
Education | Technology | Solutions

Contents SEPTEMBER 2020

cover story

features

departments

Online Communities

Follow us on Twitter:
www.twitter.com/SecurToday

Become a fan on Facebook:
www.facebook.com/SecurToday

Link to Us:
http://linkedin.com/company/security-today

STAY CONNECTED WITH COMPLETEVIEW 20/20 FAILOVER FUNCTIONALITY

Mission-critical security operations should not be left to chance. With CompleteView 20/20 Enterprise VMS, continually monitor your video system for constant accessibility and protection from failure and downtime.

Pre-configured failover servers provide secure backup for video recordings and events and transparently redirects recording servers for exceptional reliability. Failover is the security for your security system and gives customers the comfort of knowing they are protected from planned and unplanned circumstances.

Whether you deploy 50 cameras or 5000, depend on Salient for seamless failover support.

View Security Differently.
resources.salientsys.com/Failover

SALIENT™
www.salientsys.com

INDUSTRY FOCUS

With Ralph C. Jensen, Editor-in-Chief

How Security and COVID-19 Became Partners

COVID-19 has changed a lot of things about life and business Some opportunities have been challenging, other plans have been nimble exercises of security technology stepping up to the place, swinging for a home run.

In this issue of Security Today, we are publishing a host of topics, many of them include what some people in the security industry are doing to mitigate the harmful side effects of this deadly pandemic. Let's take a look.

Stephanie Weagle, BriefCam, writes our cover story, and offers a perspective about facial recognition and COVID-19. Here is where a partnership begins to form as technology meets pandemic head-on.

Weagle writes that facial recognition has also become a powerful asset for COVID-19 contact tracing for identifying those who should self-quarantine because they have been exposed to a person infected with the virus.

Cris Post, ASSA ABLOY, points out that there is no argument that the COVID-19 pandemic has forced upon us the way we interact in public spaces. He continues, that as the pandemic continues, nearly 6 million commercial buildings will be fitted to protect tenants, staff and visitors by retrofitting with hands-free door hardware.

CJ Powell, Boon Edam, writes that security and life safety have always been in lockstep. Both are fundamental needs to shield people and property from harm. The two concerns are merging as the global COVID-19 is causing a paradigm shift in operations.

We're have seen that shift in operations as people have shifted from an office job to working at home. Are you anxious to get back to the office? Think about that answer. In our office building, we are notified when someone else has notified building managers that someone has tested positive for the virus. For that moment in time, I'm happy to be working from home.

I have written a short sidebar after interviewing Chris Sessa, director of key accounts at Salient. We talked about the banking industry and how COVID-19 has changed the way we bank, and how we handle out money these days. Think about it, when was the last time you walked into a bank for a transaction?

Said Sessa, "COVID-19 has fostered many unwanted and fraudulent results." Some government entities have issued financial advisories to alert banks and financial institutions to be aware of secure financial risks.

SECURITY today

Products | Technology | Solutions

www.securitytoday.com

Volume 24, No. 6

EDITORIAL STAFF

Editor-in-Chief	Ralph C. Jensen
Content Editor	Yvonne Marquez
E-news Editor	Brent Dirks

ART STAFF

Art Director	Laurie Layman

PRODUCTION STAFF

Production Coordinator	Teresa Antonio

EDITORIAL ADVISORY BOARD

William Crews, President/CEO,
Security & Resilience Consulting, LLC, Houston
Rob Hile, General Manager,
Florida GC&E Systems Group, Tampa
Chris Lanier, LRG Inc., Jasper, Texas
Jeff Karpovich, CPP, CHPA, CSSP, Chief/Director, Security & Transportation, High Point University, High Point, NC

SALES

Brian Rendine	972-687-6761
Sam Baird	+44 1883 715 697
Peter Kao	+886-2-2949-6412

INFRASTRUCTURE SOLUTIONS GROUP

President & Group Publisher	Kevin O'Grady
Associate Publisher, Security	Ralph C. Jensen
Group Circulation Director	Irene Fincher
Group Marketing Director	Susan May
Group Website Manager	Scott Newhouse
Group Webinar Administrator	Tammy Renne

1105 MEDIA INC

YOUR GROWTH. OUR BUSINESS.

Chief Executive Officer	Rajeev Kapur
Chief Financial Officer	Sanjay Tanwani
Chief Technology Officer	Erik A. Lindgren
Executive Vice President	Michael J. Valenti

REACHING THE STAFF

Staff may be reached via e-mail, telephone, fax or mail. A list of editors and contact information also is available online at *www.securitytoday.com.*

E-mail: To e-mail any member of the staff, please use the following form: FirstinitialLastname@1105media.com

Dallas Office (weekdays, 8:30 a.m. – 5:30 p.m. CT)
Telephone (972) 687-6700; Fax (972) 687-6799
14901 Quorum Dr., Suite 425, Dallas, TX 75254

Corporate Office (weekdays, 8:30 a.m. – 5:30 p.m. PT)
Telephone (818) 814-5200; Fax (818) 734-1522
6300 Canoga Avenue, Suite 1150, Woodland Hills, CA 91367

Western Publications Association

1906 100 2006 AMERICAN BUSINESS MEDIA

ID STATEMENT

Security Today (ISSN 2572-5246) is published 8 times a year,Jan/Feb, Mar, Apr, May/Jun, Jul/Aug, Sep, Oct and Nov/Dec by 1105 Media, Inc., 6300 Canoga Avenue, Suite 1150, Woodland Hills, CA 91367. Periodicals postage paid at Woodland Hlls, CA 91367, and at additional mailing offices. Complimentary subscriptions are sent to qualifying subscribers. Annual subscription rates payable in U.S. funds for non-qualified subscribers are: U.S. $119.00, International $189.00. **Subscription inquiries, back issue requests, and address changes:** Mail to: *Security Today,* P.O. Box 2166, Skokie, IL 60076-7866, email SECmag@1105service.com or call 866-293-3194 or 847-513-6011 for U.S. & Canada; 00-1-847-513-6011 for International, fax 847-763-9564. **POSTMASTER:** Send address changes to *Security Today,* P.O. Box 2166, Skokie, IL 60076-7866. Canada Publications Mail Agreement No: 40612608. Return Undeliverable Canadian Addresses to Circulation Dept. or XPO Returns: P.O. Box 201, Richmond Hill, ON L4B 4R5, Canada.

LEGAL DISCLAIMER

The information in this magazine has not undergone any formal testing by 1105 Media, Inc. and is distributed without any warranty expressed or implied. Implementation or use of any information contained herein is the reader's sole responsibility. While the information has been reviewed for accuracy, there is no guarantee that the same or similar results may be achieved in all environments. Technical inaccuracies may result from printing errors and/or new developments in the industry.

CORPORATE ADDRESS

Corporate Headquarters:
1105 Media
6300 Canoga Avenue, Suite 1150, Woodland Hills, CA 91367
www.1105media.com

MEDIA KITS

Media Kits: Direct your Media Kit requests to Lynda Brown, 972-687-6781 (phone), 972-687-6769 (fax), lbrown@1105media.com

REPRINTS

Reprints: For single article reprints (in minimum quantities of 250-500), e-prints, plaques and posters contact:
PARS International
Phone: 212-221-9595
E-mail: 1105reprints@parsintl.com
www.1105Reprints.com

LIST RENTAL

This publication's subscriber list, as well as other lists from 1105 Media, Inc., is available for rental. For more information, please contact our list manager, Jane Long, Merit Direct. Phone: (913) 685-1301; Email: jlong@meritdirect.com; Web: www.meritdirect.com/1105

Incredible!

ASTM M50 ***Portable*** Barriers & Bollards

Available now, you can set up certified ASTM M50/P3 rated portable barriers and bollards on concrete, asphalt, compacted soils or vegetation in 15 minutes or less to provide M50 stopping power. Your people are now protected from damage by a 15,000 pound (6804 kg) medium-duty truck going 50 mph (80.4 kph). Quick deployment, multiple configurations and, best of all, unrivaled security at the highest level!

See our full line of certified crash tested portable and fixed line of vehicle access control products at **www.deltascientific.com**.

U.S. DEPARTMENT OF HOMELAND SECURITY
CERTIFIED
SAFETY ACT
www.safetyact.gov
SCIENCE AND TECHNOLOGY

Link M50 rated TB150 bollards together to create immediate protection for spans of 20 feet (6 m) or greater. TB150's contain and stop 1.2 million foot pounds of medium-duty truck.

DELTA

Visit **www.deltascientific.com** for details and specifications.
GSA 47QSWA18D003B ▲ **1-661-575-1100** ▲ **info@deltascientific.com**

Imilian/Shutterstock.com

More Secure Banking

Turning to technology as safe and trustworthy passwords

By Simon Marchand

To be successful in financial services, banks, investment firms and other institutions need to prove to their customer base that they are safe and trustworthy. Yet many still rely on passwords, PINs and other knowledge-based authentication factors—which are not only unreliable, but also insecure.

Using the Same Passwords

According to a 2019 Harris poll, 66 percent of Americans reuse the same passwords for their online banking, email and social media networks. The same survey shows that 75 percent of respondents have trouble remembering their passwords. These relics of authentication can be easily stolen, hacked or forgotten—representing challenges to both customers and institutions.

To improve both the trust of clients and the security of institutions, banks and other financial organizations must turn to new technologies to help them protect against fraud. In its many forms, AI has proven to be extremely useful when it comes to fraud prevention by allowing organizations to use algorithms to determine whether or not certain activities should be deemed suspicious. Other forms of AI, such as biometrics, can use voice and behavioral techniques to identify legitimate customers through their biological makeup or through information that can be augmented from external factors, such as the device print or location.

Here's how technology-driven solutions give companies the level of protection that their customers need and the service they expect.

Safer transactions In 2019. Banks around the world lost about $2.8 billion to fraudsters and fake transactions. With these losses amounting to billions of dollars annually, fraud can mean trouble for both the customers using these financial institutions and for the bottom lines of the banks themselves.

Fraud Solutions. Traditional transaction-based fraud solutions aren't enough anymore. Banks must have a more holistic approach, focused on detecting the individuals committing the fraud instead of focusing on suspicious transactions. It's the only way to disrupt the fraudsters' business model and to effectively reduce the financial losses from fraud.

Identify fraudulent activity. By turning to technology-based solutions, banks and other organizations can quickly identify and stop fraudulent activity before the fraudster can commit the crime. New technologies can constantly monitor customers' bank accounts and freeze the accounts or send a push notification to another device when suspicious activity is detected. This prompts the account holder to call an agent or perform a task to unlock the session, making it impossible for a fraudster to gain access — even if they manage to steal the device.

For example, with AI and machine learning in place, institutions can use models to detect irregular activity in real-time, blocking suspicious transactions before they occur. Likewise, with biometrics, it's incredibly hard for a criminal to steal a person's biological makeup — such as a voiceprint — this makes it less likely for a fraudster to get through the system. Additionally, biometrics reduces the risk of social engineering of call center agents. But biometrics also can be used to detect fraudulent interactions in the very first seconds, giving the opportunity to stop fraudsters in their tracks.

> "In its many forms, AI has proven to be extremely useful when it comes to fraud prevention by allowing organizations to use algorithms to determine whether or not certain activities should be deemed suspicious."

Better Customer Experiences

New technology cannot only protect against bad actors, but it can also improve the customer experience overall. There's no question that customers have higher expectations now than they did only a few years ago, largely because advances in technology and savvy new business models make it possible to turn historically poor experiences into seamless, satisfying and even "shareworthy" ones.

For the banking industry, authentication (such as those pesky passwords) has been a historically poor experience. Everyone has had that dreaded moment of not remembering their password and being locked out of their account, which can be incredibly frustrating and time-consuming for customers.

To remedy this fully, financial services providers need solutions that fully empower customers to have a more effortless experience in nearly every circumstance. This can begin with turning to digital methods of authentication and identification. For example, when something like your voice is your password, it eliminates the need to recall old security questions or PINS, making for a quicker, more personalized experience for the customer.

Turning to voice can also make it easy for someone like a customer service agent or bank representative to know who is calling and anticipate their needs ahead of time. For example, if a caller dials in and AI can detect that they are a senior citizen from a voiceprint, the system might be able to prioritize their call or connect them directly to a live agent rather than a virtual assistant, improving their experience and helping resolve their issue faster. This level of service cannot be matched without the addition of AI-enabled tools to current processes.

Financial institutions have been making strides to digitize operations. Still there's more that could be done—particularly by safeguarding customers and their businesses against fraud, as well as improving overall customer experiences. With potentially billions of dollars at stake every year, banks can't afford to let fraud go undetected or customer needs go unmet. By turning to technology solutions, financial organizations can set themselves up for success, keeping losses to a minimum and creating unique, safe customer interactions.

Simon Marchand is the chief fraud prevention officer at Nuance Communications Inc.

Encrypt Your Flash Drive

The safest way to store, transport confidential data

By Richard Kanadjian

USB drives are convenient devices. They are used daily by hundreds of millions of people around the world to store or transport data, much of which would be considered confidential. Chances are there are plenty of USB drives floating around your company or organization right now.

Have you ever stopped to think about the potential security threat these drives could pose? Yes, no, maybe? Well, it's a good question to ask yourself. Do your employees, contractors and visitors who connect to your network ever use them? The answer to that question doesn't really matter, because if anyone has even so much as thought about connecting a USB drive to your network, your organization is at risk.

That goes for organizations large or small, across all departments, all industries and all geographies. USB drives pose a threat, and the more unprepared you are for handling such a threat, the greater the chances are that at some point, you will have a problem. Potentially, a big problem. Do a simple Google search on data loss involving non-encrypted USBs and you will see numerous examples of organizations that did not have a solid plan in place and what the legal, financial and reputational consequences.

There are four major ways a USB drive can pose a threat:

Someone in your organization. Someone could accidentally loses such a drive that is full of data, especially what is known as Personally Identifiable Information. That happens often — way too often. Laundries often find hundred of drives in clothes they clean; this is a type of drive loss that is often invisible to enterprises yet still a potential breach.

A USB drive full of data. Important information gets stolen from your organization. People have been known to walk out of a company they were visiting carrying USB drives loaded with proprietary or legally protected information.

A trusted employee. Someone has become disgruntled and has absconded a device with confidential company data via a USB drive.

Someone in your organization. An infected USB drive has been found and, whether out of curiosity or in a noble attempt to find the owner, plugs it in. A large-scale study conducted at the University of Illinois showed that 48 percent of people who find USB drives plug them in and click on at least one file. For whatever reason they did so, the results to your network are the same if the drive is infected with malware.

So what do you do? You have several alternatives other than doing nothing. You can completely ban anyone connected to your company from ever using a USB drive at work or for work-related projects. Or, you can implement a company-wide plan on how they are to be used.

A third option is a practical compromise between the two. When policies are too difficult to enforce, and a full ban on USB drives would be impractical, encrypted USB drives make ideal solutions. Whether the drives are lost or stolen, dropped or handed to a corporate spy, encrypted USB drives will never give up their secrets, as unauthorized users cannot simply plug them in and read the data.

So what do you need to do? First and foremost, incorporate encrypted USB Flash drives and policies into your organization's overall security strategy. If you don't have such a plan and guidelines in place, your organization is at risk at every level — including failure to comply with regulations. The best time to develop an encrypted USB plan is before you need to prove you had one.

Identify the Best USB Flash Drives for Your Organization

Simple analysis of what your organization needs and recognizing there is a range of easy-to-use, cost-effective, encrypted USB Flash drive solutions can go a long way toward enabling you to get a handle on the issue of managing risks and reducing costs.

A good place to start is to select the appropriate USB Flash drive that best fits your organization's needs. Determine the reliability and integrity of USBs by confirming compliance with leading security standards such as AES 256 Encryption, FIPS 197 or FIPS 140-2 Level 3, and various other managed solution options. Also, some USB companies, such as Kingston, provide a customized option for businesses that require specific needs.

Be sure to balance company needs for cost, security and productivity. Ensure you have the right level of data security for the right price. Don't pick a drive with all the bells and whistles because you believe it to be the best if you're not going to make use of all those bells and whistles. If you don't need military-grade anti-tampering security don't pay for it, but do buy an Advance Encrypted Standard (AES) 256-bit encrypted drive for best data security. It is also a good idea to get HR and senior management involved to support your USB data-security initiatives.

Train and Educate

Education should always be the first line of defense, and explaining the different threat scenarios associated with USB drives may go a long way toward modifying bad USB behaviors.

If you don't train and educate end users, you will not have a tightly sealed data-leak prevention strategy and you are more prone to be breached. A Ponemon Institute Study regarding USB security found that 72 percent of employees use free (as in no cost, 'look what that nice person just gave me' type of free) drives they pick up at conferences, tradeshows, business meetings, even in organizations that offer 'approved' USB options.

All new and current employees should be trained as part of your company's orientation and ongoing training. Establish a training program that educates employees on acceptable and unacceptable use of USB Flash drives and the dangers of using Bring Your Own Device (BYOD) items. Take users through actual breach incidents and other negative consequences that occur when using non-encrypted USBs.

Establish and Enforce Policies

Your organization should institute policies for the proper use of electronic portable storage media, including USB Flash drives.

Here are three steps to begin the process.

- Identify those individuals and groups needing access to and/or download sensitive and confidential data on encrypted USB drives, then set a policy that allows them access.
- Document policies for your IT team and end users.
- Mandate that all employees attend training and sign an agreement post-training, so they understand the acceptable-use policies and the implications of not following guidelines.

If you don't have the right policies in place, USB drives can potentially be the downfall of your data-security strategy. Setting a policy is the first step and an incredibly important one.

Provide Company-approved USB Drives

If you don't provide encrypted USBs and implement policies that allow end users to be productive, out of necessity, employees will find a way to work around these security systems. Providing employees with approved, encrypted USB Flash drives for use in their job is an excellent way to assure that company-approved USBs are being used.

Here are a few guidelines to use in choosing the type of USB Flash Drive to give your employees:

- Proven hardware-based encryption using Advanced Encryption Standard (AES) 256. Hardware-based security provides portability and superior encryption over host-based software encryption.
- User storage space should be 100-percent encrypted. No non-secured storage space should be provided.
- Hardware-based password authentication that limits the number of consecutive wrong password attempts by locking the devices when maximum number of wrong attempts is reached.
- Your selected drive meets the FIPS standards for your particular industry or company's needs: FIPS 197 and/or FIPS 140-2 Level 3.

Manage Authorized USB Drives and Block Unapproved Devices

If you do not manage authorized drives, sensitive data can be copied onto these devices and shared with outsiders and your organization is the next statistic for data loss or theft.

If you don't encrypt data before it is saved on the USB drive, hackers can bypass your anti-virus, firewall, or other controls, and that information is vulnerable. To ensure that your data is safe, it should be encrypted before being sent out via email or saved on removable storage devices. For organizations in which confidential or sensitive data is part of your business – such as financial, healthcare and government, encryption is the most trustworthy means of protection. Following the above will provide a "safe harbor" from penalties and or lawsuits related to data loss disclosures following new regulations.

Richard Kanadjian is the encrypted USB technology and business manager of Kingston Technology.

Using AI Power

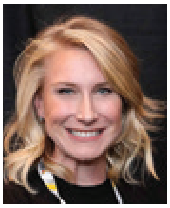
Driving efficiency and effectivity across organizations

Video surveillance is commonplace today, but many organizations don't even realize that they aren't fully leveraging the video data that their cameras capture. Traditionally, law enforcement and physical security teams use video cameras to monitor areas in real-time and to review footage to glean evidence for post-incident investigation.

Given that staff resources and time are usually limited, it is not realistic to monitor all cameras in real-time, or to manually review all available footage resources post-incident. Even if they have the time, human observations are subject to error or oversight. As a result, most video footage is never viewed or put to practical use, so many organizations miss out on this veritable treasure trove of valuable information.

Progressive organizations have realized that they can, and should, get more value from their video surveillance networks and footage. In recent years, Video Content

"Progressive organizations have realized that they can, and should, get more value from their video surveillance networks and footage."



By Stephanie Weagle

Zapp2Photo/Shutterstock.com

Analytics software powered by Artificial Intelligence (AI) has emerged as a crucial and complementary technology for video surveillance, because it allows organizations to harness the valuable data in video footage that would otherwise go unused.

Video content analysis allows surveillance security teams to quickly review footage from past incidents, increase situational awareness and response time to evolving situations, and obtain trend data for developing strategies and making data-driven decisions to prevent future problems. The software benefits many industries and is fast becoming a standard part of technology suites, not only for corporate security teams and law enforcement agencies, but also for business groups across organizations.

Driving Agile and Effective Security

Depending on the environment, security and enforcement teams juggle an array of responsibilities, from reducing theft to increasing public safety, or solving crimes. With AI-backed analytics, users can accelerate investigations by searching objects and events of interest with speed and precision.

Operators can filter objects or scenes according to classifications such as male/female, adult/child, vehicle type, and lighting changes, as well as appearance similarity, face and license plate recognition, color, size, speed, path, direction and dwell time.

This is enabled by AI-driven technology and Deep Neural Network training, which exposes the machine to tagged data to teach it – much like the way a human learns – how to identify objects in video. This enables data to be searched, aggregated and leveraged for triggering alerts. By translating live or archived video into structured data and extracting rich metadata for object extraction, recognition, classification, and indexing activities, video intelligence solutions transform the data into searchable, actionable and quantifiable intelligence for driving investigations, real-time response, and long-term planning.

The ability to forensically filter video based on extensive object classification and recognition empowers the video investigator to pinpoint the most relevant data based on distinct search combinations, such as querying for a person of interest wearing blue jeans and brown coat, heading east between the hours of 4 p.m. to 6 p.m. on a specific date at a particular location.

When such search and filter capability is also extended to the field via mobile technology, officers at the scene of a crime or emergency can quickly search on-site video based on witness descriptions, to jumpstart the investigation before returning to a real-time crime center. Whether in the field or an office, the ability to rapidly search footage across multiple video cameras in a network dramatically decreases the time-to-target and saves hours of investigation and suspect tracking – ultimately preventing crime and freeing up staff to pursue other critical duties.

Improving Situational Awareness with Real-time Alerts

AI-powered video content analytic software is not only for reviewing past events; it also enables organizations to proactively respond to situational changes in an environment, via real-time alerts. Using the same set of object classes and attributes, a video intelligence system can be configured to trigger rule-based, real-time alerts when pre-defined conditions are met. By benchmarking expected activity and by detecting anomalous behavior, users can create alerts for abnormal conditions, such as lighting detected after-hours or a car idling in a pedestrian-only zone.

Video analytics operators can define any number of conditions that require customized alerts- such as crowding and dwelling – for increased situational awareness and proactive and preventative response to a variety of problems.

For example, during the COVID-19 pandemic with its social and physical distancing recommendations, alerting is crucial for detecting and mitigating crowding in facilities of all types. Similarly, dwelling can also be an indication of a problem – whether a medical emergency or an intent to commit a crime – and real-time dwell alerts can be set up to notify when an object or a person has been detected in one spot for an extended duration of time.

Mitigating Risks, Monitoring Compliance

Crowding is a common security and customer experience challenge -— whether in a retail store queue or at an airport security gate – and, therefore, it's useful to have count-based alerts, which can be configured to trigger whenever the number of objects or people in a particular space exceeds a pre-set threshold. With alerts, operators can proactively detect the early stages of congestion, crowding, or even security breaches when unusual numbers of people are identified in an off-limits area, and quickly assess and preventatively respond to events as they unfold.

One particularly timely example of people counting analytics, is the detection of and alerting for social distancing violations in grocery stores, manufacturing facilities, warehouses and worksites of all varieties. In addition to real-time alerts, managers can also leverage people counting, occupancy and even proximity data to compile reports, dashboards and heat maps for documenting compliance with public health mandates or pinpointing problem hotspots where recommended safety protocols are typically not observed, in order to develop solutions to combat these challenges.

Dashboards and heat maps based on video analytic data can also demonstrate the areas of a private business or public setting that have the highest occupancy and traffic rates – and the peak times of day – to pinpoint where social distancing measures may be difficult to enforce. Municipalities may leverage this comprehensive operational, activity and demographic intelligence to deploy law enforcement to certain city streets or parks where there are high volumes of pedestrians.

Beyond the coronavirus crisis, the ability to detect both patterns and anomalies, empowers organizations to enforce compliance and respond to violations of other important work safety mandates, such as wearing proper safety gear from hard hats to face masks in a work zone. Again, this analytic filter can be used for searching video and triggering alerts; but, over time, the video analytic trend data also can be visualized and analyzed for making intelligent decisions and protecting workers and visitors from everyday hazards.

Face and License Plate Recognition

Often, event prevention and resolution can be accelerated by locating or identifying a specific person or vehicle – whether a criminal suspect, VIP or, in the case of the global pandemic, a self-identified individual who's contracted the illness. In cases where operators are looking for an identifiable person or vehicle, face recognition and license plate recognition capabilities make searching, alerting on and analyzing video more focused and quick.

"In the wild" face recognition technology relies on watch lists of digital face images to drive identification, video searches and alerts, from watch lists of suspected criminals to those of personnel authorized to enter a sensitive facility. Once a face match is detected, human operators can investigate or evaluate the scene, validate the match and determine how to respond, whether to continue closely monitoring or confronting the individual.

The same principle is true for cars. Law enforcement can, for instance, create watch lists with the plate details of stolen vehicles and trigger alerts whenever a matching plate is detected. Another application is for detecting unauthorized vehicles – especially those associated with previous suspicious or criminal behavior – on a secure premises or in sensitive loading dock areas.

Face recognition has also become a powerful asset for COVID-19 contact tracing for identifying those who should self-quarantine because they have been exposed to a person infected with the virus.

In a workplace, for instance, an employee can disclose his or her diagnosis to the employer, who can then use facial recognition to identify the employee throughout the work environment over the 14 days prior to the diagnosis. The employer can then identify which other employees or visitors may have had contact with the individual and mitigate further risk by instructing relevant people to self-isolate. This can be done without compromising the anonymity of the infected employee.

Of course, in settings or jurisdictions where there are legal restrictions or physical limitations to using face recognition, it's helpful to have broader, non-personally identifiable search and alert filters, so operators can apply appearance similarity criteria rather than face recognition – or, in the case of vehicles, license plate recognition.

Distilling Big Data for Operational Intelligence

One of the most significant advantages of video content analytics is that it empowers users to detect not only the granular details – with outstanding precision and speed – but it also can capture and deliver video metadata that has been aggregated over time.

Video content analytics systems provide business intelligence about occupancy, traffic, and dwell patterns. These data visualizations not only help managers identify recurring problems or criteria for expanding real-time alerting and improving response times, but it also drives decision-making by providing accurate insights and trends. Empowered by quantifiable data and trends from video, teams can make better operational decisions based on that actionable intelligence rather than relying on memory or anecdotal observations.

Trend data is important for planning and strategizing how to optimize visitor or customer experiences and business goals.

For example, marketing, operations and security teams in a large event venue or conference center can evaluate historic pedestrian and vehicular traffic to understand where traffic bottlenecks occur, or which entrances are more effective for displaying informational or retail kiosks. In a retail environment, operators can map common customer paths, object interaction, and dwell times. This helps users identify crime hotspots, optimize traffic flow at major traffic interchanges or store locations, track crowd demographics, size and movement patterns; design more effective floor plans or parking lots; and track employee compliance with safety regulations.

To overcome ever evolving challenges, today's security and operations managers need better technologies for ensuring public and workplace safety and productivity. AI-powered video analytics software drives increased efficiency and effectivity by enhancing surveillance systems most organizations are already using. With flexible architecture options for deploying video analytics in the cloud or on-premises, video analytics technology is more accessible than ever to meet the budgetary, staff and timeline requirements of each individual business. Given that most security organizations already invest in video surveillance, video content analytics is a logical way to maximize that investment with measurable results.

***Stephanie Weagle** is the chief marketing officer at BriefCam.*

IT STARTS WITH LISTENING

WE BELIEVE THE KEY TO SOLVING ACCESS CONTROL PROBLEMS IS COLLABORATION—between our customers and our innovation specialists. It involves listening, observing and analyzing—turning the full force of our experienced team to your challenge. Tell us about your toughest access control problems. Our team is ready to listen and create a solution for you.

CyberLock®

sales@cyberlock.com | 541-738-5500 | www.cyberlock.com

A Hands-free Environment

How to prepare for the new normal

By Cris Post

No one will argue that the COVID-19 pandemic has dramatically changed the way we interact in public spaces.

Since the pandemic struck, and the United States has been struggling to adapt to the "new normal," facility managers in organizations across all industries and sectors have been scrambling to implement effective, efficient solutions to minimize the risk of exposure for their employees, visitors and patrons.

As workplaces implement new processes, including making schedule changes, facilitating cohort rotations or reconfiguring work areas to achieve the recommended six feet of separation, leaders are looking for solutions that fit their specific needs – ranging from low-to-high tech – to keep their staff safe in a variety of environments.

One of the most frequently touched surfaces is door hardware, so it should come as no surprise that alternatives like hands-free door openings can minimize a multitude of skin-to-surface touch points throughout the day. Regardless of future regulations, reducing the number of contact points in a facility will be an effective way to minimize future germ spread.

As there is no "one size fits all" when it comes to ensuring a building is a completely touchless environment, facility managers must assess and identify door opening solutions that meet the specific needs of their spaces to minimize the spread of germs and bacteria.

Automated Openings

Automated openings like revolving doors, swing doors or sliding doors, offer stylish touch-free convenience for building entryways that are high risk areas for the spread of viruses – simply based on the sheer number of people passing through them each day.

Modern automatic sliding door systems can be customized for all uses, tastes and architectural styles, from rugged aluminum-framed door systems for demanding high traffic areas, to all-glass systems for unobstructed views, and even curved sliding doors for elegant entrances.

Key Card or Mobile Entry Systems

Managing secure entry with key cards or mobile entry systems will be integral for facility managers to monitor access to areas within their buildings. With heightened concerns around adjusting capacity to allow for the required social distance in spaces like lobbies, elevators and conference rooms, understanding and tracking not only how people move about the building, but also which areas are "hot spots" for activity, is critical to upholding occupant health and safety.

Key cards and mobile entry systems are easy to use and allow for access to multiple areas with a single card. Additionally, with the ability to grant and remove access rights remotely, facility managers can control access as remote workforces return to work in various shifts and in different numbers.

Halfpoint/Shutterstock.com

Hands-free Arm and Foot Pulls

Now more than ever budgets are tight, but facility managers need to take urgent action to retrofit existing hardware to dramatically reduce skin-to-surface touch points, like door handles and pulls for bathrooms, entrances and offices, as populations begin to return to work and public spaces.

Hands-free arm and foot door pulls are cost-effective options for low-touch door operation for both pre-existing and new openings.

Push/pull hardware enables occupants to open doors with a nudge of the hip. Arm and foot pulls offer a method of opening doors without grasping hardware by the hand. Best of all, these hands-free solutions can be quickly and easily retrofitted in existing buildings. In addition, they support ADA standards and regulations to ensure all openings remain accessible to everyone.

> "Regardless of future regulations, reducing the number of contact points in a facility will be an effective way to minimize future germ spread."

Radio Frequency Sensors

Radio frequency devices automatically open doors when an individual comes within the range of the door operator's sensor. Some receivers can accept up to 30 transmitters, making these devices ideal solutions for spaces where wave switches are not practical, or for situations where individuals regularly pass through specific doorways, such as maintenance workers or luggage porters.

Wave-to-Open Switches

Wave-to-open switches, coupled with low energy door operators, allow occupants to easily move through a building without transferring germs.

The sensors in wave-to-open switches detect hand gestures within four inches of the switch and are highly precise to avoid false activation. They can be programmed to hold a door open up to 30 seconds allowing multiple people to move seamlessly between conference rooms and offices without worrying about touching and transferring germs.

Hassle-free Upgrades

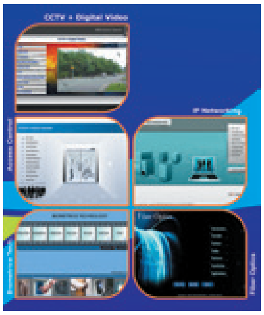
All types of swing doors can be upgraded to open automatically using a low energy door operator paired with a wave-to-open switch, RF device, and/or remote control fob. And, these devices can work alone or in concert with fire alarm, access control and other building automation systems.

The latest door operators are designed to be installed by one person on single or double doors. They address a critical pain point by enabling integrators and facility managers to quickly and easily program and adjust door operator settings using a WiFi-enabled smart device.

In addition, if multiple door operators exist in the same facility, installers can simply save and port over settings to other units, eliminating the trouble of setting up ladders and removing device covers.

As the pandemic continues to evolve and as our nation's nearly 6 million commercial buildings prepare for a new normal, the question of how to protect tenants, staff, and visitors will continue to be top of mind. Limiting contact and exposure by retrofitting with hands-free door hardware is an important line of defense in rebuilding trust and reducing risk for building occupants and guests. Investing in these solutions to minimize germ spread will deliver both immediate and long-term tenant health and user experience benefits.

Cris Post *is the general manager of Rockwood Products*



Do you have a plan for the Sunset?

Alula does.

www.Alula.com

alula™

Professional Smart Security

The Evolution of Risk

How security entrances address vulnerabilities today

By CJ Powell

Risk prevention has always been a fundamental part of business planning and operations. And while the various forms of protection available have evolved over the years, so also has risk.

About 20 years ago, professional security was mostly limited to night watchmen, armored trucks and closed-circuit video cameras wired to VCRs. The main entrance to all but the most secure government or sensitive facilities would encompass nothing more than a set of glass doors and perhaps a receptionist visually checking ID cards from behind a desk.

Events between 1990 and 2001 changed those ideas forever. The 1993 bombing of the World Trade Center, the Enron scandal leading to a multitude of compliance laws, the shootings at Columbine High School and ultimately the events on 9/11 ushered in a new age of security that now encompasses cybersecurity as well.

Security and life safety have always been in lockstep, as they are both fundamental needs of organizations to shield people and property from harm. Today, these two concerns are merging in an unprecedented way as the global COVID-19 pandemic is causing a paradigm shift in operations. Now it is also necessary to protect ourselves from the handles, buttons and other structural components of buildings we regularly need to touch for entry and exit.

PROBLEMS PRESENTED AT ENTRY POINTS

The entry has always been one of the most vulnerable and critical points in a facility. Whether the concern is compliance, cybersecurity, terrorism, violence, theft or any of the hundreds of other risks facing businesses, it is of fundamental importance to secure any location where people can enter a facility.

From a security perspective, the objective is to keep any unauthorized individuals out of the building or off the campus. Further, within each building, the objective is to ensure that any individual division, area, wing or room can only be entered by those who are authorized to be in that place at that time.

From a life safety perspective, since the entry is also the exit, it needs to provide the means for rapid and safe egress in case of an emergency. From a health perspective, many organizations are now adding the requirement that entry and exit be "touchless" as well.

Over the years, as risk evolved, the security industry's approach to entry began to change along with it. Better locks were developed, and access control readers were placed at doors both outside and inside facilities, requiring a card swipe or tap to unlock the door. As the technology matured, the products became more sophisticated, with Wi-Fi locks, mobile credentials and biometrics among the developments.

THE SHORTFALLS OF SWINGING DOORS

While these advancements were significant, they did not address an important security shortfall. The majority of facility doors, both exterior and interior, are still standard swinging doors. There are many different form factors and types of locks for these doors, and the software that manages their locking and unlocking has become more advanced.

However, the doors themselves still work in the same way as they always have; when unlocked, they swing open and then close again. They may close, and/or re-lock, automatically – but once they are open, there is no barrier to entry for one or more people.

Even if a door is held open for only a few seconds, it fully negates the security function of the doors, since multiple unauthorized individuals can enter this way. There are many ways this can happen. A person may slip quickly through behind another, while "pretending" to search for their ID card. One authorized person can enter and pass their credentials back through the door for a second person to use. Or the door may simply be held politely for the next person to pass through.

Placing security officers or installing tailgating analytics technology at each entrance can help to mitigate these risks. However, guards can be misled by a false ID or a good story. For example, "white-hat" penetration testers have proven that a clean-cut man wearing khaki slacks and a polo shirt, carrying a ladder and a clipboard, and claiming to be there to provide some kind of maintenance, will almost always be allowed to enter without credentials. Most tailgating detection technology such as sensors with alarms, is reactive, alerting management only after the unauthorized person has already breached the facility.

Also, of course, none of this addresses the issue of virus transmission from touching surfaces that others have touched.

SECURITY ENTRANCES DELIVER A SOLUTION

Security entrances can solve many of the problems of entry while offering numerous additional benefits. Unlike standard swinging doors, a security entrance, such as a turnstile with barriers, a security revolving door or mantrap portal, is designed to allow entry for only one authorized user at a time.

Some types of security entrances require local supervision and operate as a deterrent, while others work in such a way to prevent any type of tailgating. Regardless of type, compared to a swinging door, they are definitely a physical security upgrade due to their ability to significantly reduce the risk of infiltration.

Most important at this moment in time, optical turnstiles with barriers, security revolving doors and mantrap portals are excellent candidates for touchless entry. New integrations with facial recognition technology, powered by artificial intelligence (AI), are enabling authorization and entry for individuals based on biometric credentials – without the need to touch a handle, button or access reader.

With this technology in place, a security entrance can authorize an approaching individual from a few steps away and automatically move the turnstile barriers or door wings to enable a safe and healthy entrance to the facility.

ADDRESSING RISK IN A NEW WORLD

The meaning of the word "security" has irrevocably changed in the past two decades. Organizations, campuses and corporate stakeholders are now at risk in ways that would have been unimaginable even two years ago.

***CJ Powell** is the vice president of sales at Boon Edam.*

The Power to Work Smarter

ASSA ABLOY

The New Securitron AQL Series Intelligent Power Supply

What if you could service your clients quickly from practically anywhere?

With Netlink™ Network Monitoring from LifeSafety Power, the new Securitron AQL Series gives you the power.

Remotely analyze, control and test your customer's power system and batteries from your desk or smartphone.

Notifications alert you to problems before they happen, allowing you to take a proactive approach to customer care and maintenance. Now that's smart power.

LIFE
MagnaCare
Warranty

Learn more at assaabloyesh.com/aqlpower

ELECTRONIC SECURITY HARDWARE HES | Securitron

800.626.7590 | assaabloyesh.com

Experience a safer
and more open world

The Rise and Sophistication of Mobile Apps in Physical Security Sector

Technology helps support security, safety and emergency management programs

By James K. Lantrip

Safety and security risks are everywhere including the office, schools, concerts, retail malls and hospitals. However, security professionals, who are tasked with protecting the public, can't be everywhere at all times and they require timely information in order to prevent potential incidents. Security professionals are trained to know when a person, or group of people are acting suspicious. They see, hear and learn things every day that could help prevent a safety or security incident from happening. In fact, many incidents have early-warning predicators that are observable and these incidents can help be prevented with the right technology tools and techniques.

David MG/Shutterstock.com

"Security professionals are trained to know when a person, or group of people are acting suspicious."

While well-trained security professionals will always remain the steadfast foundation of security programs, advancements in technology that are accessing easy-to-use apps can enhance their ability to gather intelligence and protect the facility. Blended personnel and technology solutions can create efficiencies, target security efforts and give security directors the power to make informed decisions that deliver even greater return on their security investment. From tour management systems and access control systems, to mobile reporting and facility-wide alert systems, technology helps support security, safety and emergency management programs in many ways.

Data collection. Tour management systems using mobile devices allow security officers to capture data in real time. Automated instructions and questions can be set up for security professionals to answer at each checkpoint, such as entrances, escalators and emergency callboxes. For example, a security professional on daily tours can be prompted monthly to document fire extinguishers' inspection dates, essentially combining two tasks and providing additional value.

Streamlined reporting. Data obtained at checkpoints can be easily analyzed through simple reports to identify operational risks. These risks might include policy issues, such as specific doors repeatedly being left unlocked; safety issues, such as recurring hazards at specific elevators; or maintenance needs, such as inoperative callboxes.

Actionable information. Technology supports security strategy and enables optimized security officer deployments, precise post orders, directives for specific threats and countermeasure deployment to enhance security in areas where it is needed most. For example, incident management systems can identify sites and time ranges of incident volume based on historical data in the system. This can help determine security staffing levels and result in safer facilities and improved risk mitigation, reducing costs to the facility.

The walls between physical security and cyber security are coming down with worlds converging. Today's security professional accesses high-performance apps from their mobile phone or tablet which enhance productivity, accountability and access to vital information. Consider a security warning about a predator on campus which is shared with a physical security team who are able to take action and ensure that a threat doesn't become a tragedy. What about an access control system that registers an employee physically swiping access into their Washington, D.C. office while their cyber presence is being registered in Jacksonville, Florida? Or telemetry collected from cameras which alerts to suspicious activity which empowers on-the-ground security professionals to take action? Security professionals are able to gather all this information via the newest and most efficient breed of mobile apps available.

AI AND APPS

Integrated solutions are going beyond the outdated "detect and respond" model of risk management to become an ecosystem that provides a comprehensive safety and security solution with artificial intel-

Winsted®
Control Room Consoles

ligence at its core. An integrated workforce ecosystem ensures reduced liability and enhanced reputation that amplifies the effectiveness of onsite security.

For example, HELIAUS® is able to transform data into actionable insights, and take the guesswork out of where the security team needs to proactively mitigate risk from incidents and improves response. This advanced artificial intelligence platform is designed to improve safety and reduce risk by enhancing onsite guarding services.

It's not an either or between technology and people; it's about arming security professionals to work with technology. Today's workflows task security professionals via text and email. AI systems interface with a company's monitoring and response centers (MaRCs) in which remote video monitoring data and video analytics data are accessible from the portal and accessed via phone or tablet. These technologies can have data sources that include information from IoT sensors, drones, robots, along with cameras and other sources.

Our business ecosystems today include monitoring and response centers that provide an abundance of tools and technologies including threat intelligence platforms, remote video and alarm and event monitoring to traditional alarms and remote audio and positioning based patrol route management. Effective communication is critical to maximizing the efficiency and productivity of cutting-edge ecosystems to achieve optimum outcome that ensures enhanced safety and security.

MASS NOTIFICATION APPS

For vital, time-sensitive messages, security professionals rely on mass notification apps which allow them to engage in real-time, one-way interactions with any number of people using a text

alert voice message, email message, app push, digital signage and other customized channels system so that the message can be shared instantly.

Security professionals and the administrators are able to send notifications to thousands of people within seconds. They can initiate requests for help, reply to messages and actively monitor the well-being of their customers from their front-line perspective. Some respected mass notification apps include Everbridge, LiveSafe, SafeZone, AlertMedia, CallMy and ReGroup Mass Notification.

Why are mass notification apps "de rigueur" in our modern world?

Consider these scenarios. Several employees headed to the corporate center have disembarked from a commuter train and are walking through a transit center heading east to the parking structure where their cars are located. However, when they arrive at the ground lobby, their smartphone receives an automated text message alerting them that there was a chemical spill near the east side exit of the building. The text message guides them to an alternative and safer exit to avoid being near a contaminant.

Or perhaps a gunshot is heard on a college campus. All students and faculty receive a message about the location of that gunshot and whether they should shield in place or move to another, safer location.

Mass notification alerts could be used to protect people from any number of hazards and emergencies — a flash flood warning for people traveling near a suddenly dangerous roadway or a wildfire alert where flames could be creeping dangerously close to a road or housing community. These mass notification apps go beyond two-way communication to provide a full critical communications cycle that initiates an organization's emergency response plan's predefined crisis communication plan.

Many of the mass notification apps include the ability for students or employees who are working late to check in on their app to request a security escort to walk them to their car or dormitory.

The advent of COVID-19 pandemic presents an immediate need for security professionals and their communities to be able to instantly communicate with each other. For example, if an employee, student, teacher or contractor is found to be positive with the virus, the security professionals need to roll out an immediate containment plan.

LIVESAFE RELEASES COVID-19 APP

In March 2020, LiveSafe Inc. announced a free, limited version of its safety and two-way communications app, as well as the platform's Command and Communications Dashboard, available to any business, college, university or healthcare institution that needs a way for employees or students to anonymously communicate their concerns and receive important information about the COVID-19 outbreak.

The COVID-19 Safety Resources App enables members of an organization's workforce or student body to engage in two-way communications with their COVID-19 coordination or response team. Rather than relying on email or emergency notification systems, the LiveSafe Platform offers a discreet way for organizations to engage their workforce and students during a time of limited resources and rapidly changing information.

"We are all in this together and we are stronger when we come together as communities to address critical safety, security and health concerns," said Carolyn Parent, LiveSafe president and CEO. "In a dynamic environment like the COVID-19 situation, being able to provide accurate information, mitigate your employee's concerns, and get inbound information about their status can be overwhelming to safety and security teams. LiveSafe enables two-way chat and broadcast, and offers needed anonymity so you can quickly identify who needs help and deliver accurate information to your workforce or student population."

APPS AND COST-SAVINGS

Using HELIAUS, a major Hollywood production studio was able to identify and address their workplace hazards with $657,000 in potential savings due to the improved reporting of slip-and-fall hazards. A perishable foods manufacturer saw over $55 million in potential losses avoided at a single site due to this AI platform.

A Texas hospital plagued with homeless entering the facility saw a 200 percent drop in security incidents with increased staff, visitor and patient satisfaction. A Washington DC landmark property realized $67,064 in savings from improvement to fire safety measures driven by this AI platform that directly reduced the risk of fire from ovens and heating elements accidentally being left on.

Today, the walls between manned guarding, staff and technology will come down leaving us with an ecosystem that allows ALL things to cooperate at light speed which ensures that we're considering everything we need to consider, and bringing all these resources to bear in a way that drives better outcomes.

James K. Lantrip *is the senior vice president of operations for Allied Universal Technology Services.*

SECURITY BEGINS AT THE TIP OF THE SPEAR.

Today, across the country, **SAGE Integration** is not just protecting the people, facilities, and reputation of some of America's most risk-conscious companies. Additionally, **SAGE**'s national network of team members is advancing the intelligence and integration of security technology.

As legacy players stall against the headwinds of a fast-paced future, and local practitioners fail to address the global risks of the enterprise companies, we invite you to get to know the empowered team at **SAGE Integration**.

+35 MAJOR U.S. METRO AREAS WITH ACTIVE IMPLEMENTATIONS

+19K INSTALLER SPECIALISTS ACROSS NORTH AMERICA

+30 YEARS OF EXECUTIVE SECURITY INDUSTRY EXPERIENCE

24/7 SERVICE AND RESPONSE SUPPORT NATIONWIDE

SEATTLE · CHARLOTTE · NEW YORK CITY · HOUSTON · PORTLAND
SACRAMENTO · SAN DIEGO · AUSTIN · HARTFORD · BOSTON
LOS ANGELES · ORANGE COUNTY · LAS VEGAS · PHEONIX
KANSAS CITY · DENVER · RALEIGH · ALBANY · TORONTO · CHICAGO
MINNEAPOLIS · NASHVILLE · CLEVELAND · DES MOINES · DALLAS
WASHINGTON, D.C. · TAMPA · ATLANTA · OKLAHOMA CITY · SAN
ANTONIO · NEW ORLEANS · DETROIT · PITTSBURG
JACKSONVILLE · MIAMI · VIRGINIA BEACH

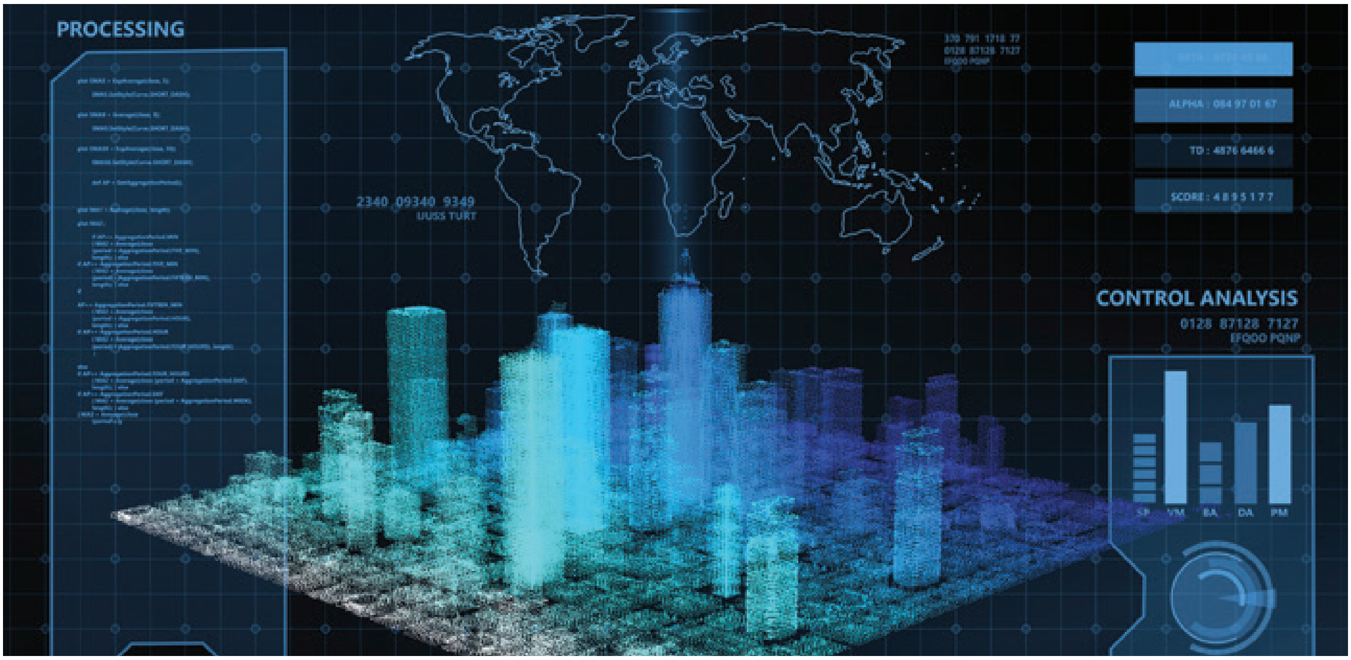
WWW.SAGEINTEGRATION.COM

SAGE integration

Coordinating Emergency Communications

How IoT can drive efficiency and response

By Kevin Taylor



thinkhubstudio/Shutterstock.com

One of the many lessons learned from the Smart Cities movement is that you can achieve significant improvement in community safety and resilience when you use network technologies to facilitate communications and data sharing. Information gets to responders more quickly and comprehensively which leads to more streamlined processes and better decision making in the field.

When walking through a modern Real Time Crime Center (RTCC), it is easy to become fixated on the huge video walls, workstations with elaborate dashboards, and images streaming into the center from cameras across the city. But the real value of these centers is not the eye-catching displays, it is the aggregation and efficient sharing of data with multiple stakeholders.

The data sources collected into the RTCC are not limited to cameras. You will also find information streaming in from other devices like license plate readers alerting when a registered stolen vehicle is detected, radar triggering notification of illegal trash dumping, and audio sensors detecting the discharge from a firearm.

All these data sources help operators in the center focus on areas where conditions indicate a likely negative outcome for the community. There are dynamic mapping applications assisting operators in geolocating events, technology assets and personnel in the field. The center might even be using analytics based on artificial intelligence to help compile raw data and quickly push critical information to responders.

The goal is to gather the most complete picture possible of what is happening on the streets of the city, so responders can work smarter – planning strategies on the way to a scene so they can perform more effectively once they arrive.

> "… the real value of these centers is not the eye-catching displays, it is the aggregation and efficient sharing of data with multiple stakeholders."

"Aggregating all this technology into one system is an exceptional force multiplier. We've learned that the more situational awareness we can get to our responders the better for everyone," said George Brown, IT/COMMS manager for the New Orleans Real Time Crime Center.

REDUCING REDUNDANCY WITH STREAMLINED WORKFLOW PROCESSES

This new operating model is a sharp contrast to how 911 calls were managed in the past. Previously, when a 911 call came into the Public Safety Access Point (PSAP), the operator would pass the call on to a dispatcher who would send an appropriate responder – police, fire or medical – to the caller's location. The information that reached the responder seldom contained more detail than the basic nature of the call. The inability to move data consistently throughout each step created knowledge gaps, requiring responders to recollect data that was previously provided, but not transferred. With an RTCC solution, much of this redundant activity is eliminated.

Smart city solutions are built on scalable, open-standards platforms which allows them to accept data directly from other open-

Maximum Weather Protection

Indoor and outdoor camera products since 1998

New Product Alert
DomeWizard™
ELEVATED MULTIMODE CLEANING SYSTEM
10 FEET, 25 FEET, & 40MAX FEET
Mode 1
Mode 2
Mode 3
1
2
3
Patented

New Product Alert

DomeWizard™

ELEVATED MULTIMODE CLEANING SYSTEM

10 FEET, 25 FEET, & 40MAX FEET

Maximum Cleaning

Designed for max service revenue, cleans more products, and no ladder required.

3 Modes

1 2 3

Patented

S-Type

IP66

STXL

S-Type Extra Large

Protection for Camera and Long Lenses

IP66

D2

IP68

D3

IP68

HD12

IP66

B.O.B.

Bi-Ocular Box

IP66

BR-Q61

Axis Q61 Series Integration Kit

Made in USA

dotworkz.com

(866) 575-4689

dotworkz systems

Fortified outdoor camera housings and accessories standards sources. With all data streaming into a single information repository, these solutions reduce redundant data collection and entry. Authorized users do not need to log in and out of multiple systems to input and access critical information.

They can pull up camera views, map overlays, analytics, and other applications all on a unified screen -- a significant time saver. Equally important, they can push critical situational information and visuals to responders' mobile devices before they arrive on the scene and provide ongoing details as more information streams into the command center.

By leveraging all their technologies to create a logical and consistent workflow for emergency response, smart cities can maximize the value of data, drive departmental efficiencies and allow cross-departmental collaboration which ultimately leads to a safer community.

With a large repository of data and analytic tools at their fingertips, agencies can also accelerate the detection of patterns that previously might have gone unnoticed.

When asked about the Hartford Capital City Command Center (C4), Johnmichael O'Hare, a former member of the Hartford Police Department, said, "While we initially focused on solving crime, we're also finding that our smart city solution can help us recognize areas of the city that might benefit from reengineering." Some of those discoveries have ultimately led to footbridges being constructed over busy roads and new lanes designated for bicycles along certain corridors.

SAVING LIVES WITH NATURAL DISASTER WARNINGS

This comprehensive approach to collecting and optimizing data is especially valuable when it comes to community resilience in the face of natural disasters. In those situations, timely alerts and rapid reaction often translate into lives saved.

That is why cities prone to flooding, hazardous road conditions, earthquakes and other catastrophic phenomena often integrate environmental sensors into their smart city solutions as part of their emergency preparedness program. With the addition of modern communication assets such as dynamic message boards and mass notification systems, these early warning tools help cities be more proactive in initiating emergency public safety protocols.

Anticipating flood evacuations. In lowlands and coastal regions prone to tropical storms, water level sensors linked to network video cameras monitor rising ground water and send alerts about potential flooding, allowing the city to initiate pre-planned evacuation procedures before routes become impassable.

Responding to hazardous road conditions. Intelligent cameras with onboard analytics can function as Environmental Sensor Stations to detect weather activity – such as torrential rain, snow, sleet, or ice – that will likely lead to hazardous roadway conditions. With early detection, agencies have time to divert traffic to less risky routes, close specific roadways, or issue shelter-in-place advisories for affected areas.

Alerting public to impending earthquakes. In areas prone to earthquakes, underground sensors can provide early detection of seismic activity. They are generally tied into mass notification systems that use IP speakers in public spaces to broadcast warnings for the community to seek safe shelter before the quake hits.

WHY IP-BASED EMERGENCY COMMUNICATIONS SOLUTIONS ARE SO EFFECTIVE

An emergency communications solution based on IP technologies makes it possible to integrate multiple agency sub-systems into a unified user experience. It allows a city to drive a more efficient and comprehensive flow of information to those who need it, when they need it. These solutions are elastic in nature, easily scaling up or down to fit the needs of a specific situation.

They can be set up to regularly self-monitor and automatically notify administrators of failures and outages as they happen. This ensures that problems are discovered and corrected before an event response when reliance on complete system operability is critical.

Describing his experience with his own city's real-time command center, Maj. Neil Klotzer of the Atlanta Police Department said the comprehensive solution "demonstrates that working together, we can build a safer, more security city for everyone. And we can do it while respecting the right to individual privacy."

With ever-increasing challenges faced by public safety and emergency preparedness officials, creating a cohesive emergency communications network that fosters interagency support and sharing of resources is both a valid, and a valuable, path forward.

Kevin Taylor *is the business development manager, Smart Cities, Axis Communications Inc.*

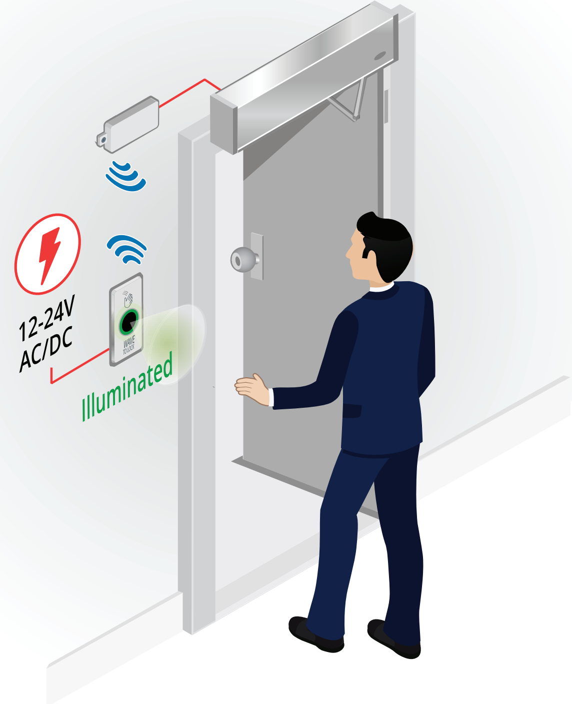
SURE·WAVE™
BY CAMDEN

TOUCHLESS: Designed For Retrofit

CAMDEN
DOOR CONTROLS

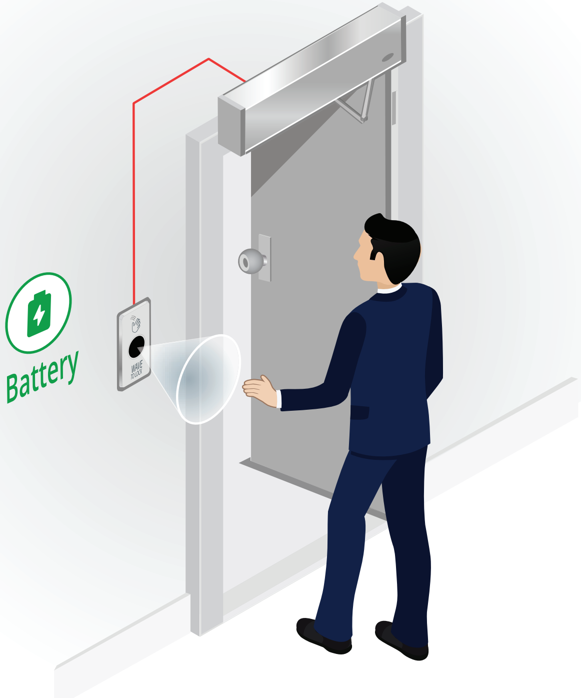
Opening New Doors to Innovation, Quality and Support!

Call: **1.877.226.3369 / 905.366.3377**
Visit: **www.camdencontrols.com**



CM-331 Series: Reuse 2 existing wires for power and install an optional CM-TX99 plug-in wireless transmitter to activate the door opening!

– OR –



CM-333 Series: Reuse the 2 existing wires to activate the door opening and battery to power the switch, with 2 year battery life!

???/Shutterstock.com

The Threat from Within

Protecting banks during the challenge of COVID-19 and a reduced staff

By Kami Dukes

Just as banks use every tool at their disposal to maximize revenue opportunities and manage their ledger, they must take the same approach when it comes to security. New challenges with COVID-19, banks operating with a reduced staff and employees working from home require an updated and more diligent security plan. Insider threat programs are a key component to an overall security plan.

While financial institutions implement some level of security, they can improve their security and insider threat programs leveraging the latest security technologies. Cross-department collaboration, a practice that challenges organizations, is an extremely helpful part of the solution but is often the hardest to execute. Combining the right mix of technology and security staff will better protect financial institutions from insider threats and help meet COVID-19 guidelines.

The biggest risk to financial institutions is the possibility of bank employees accessing private user account data, including account numbers which can be printed, emailed, saved and be sold to bad actors for a high dollar amount. Most banks have deployed an access control system to manage access throughout their complicated environment. Access control systems collect large amounts of employee access data on a daily basis. While the amount of data collected is overwhelming and difficult to manage, it is extremely useful when trying to identify potential risks.

An analytics system can process access control data and assist with insider threat and COVID-19 challenges. Deploying an analytics system alongside an access control and identity management system can help leverage data to identify risks through anomalous behaviors by tracking an employee’s access history and behavior patterns.

HOW ANALYTICS SYSTEMS WORK

People are creatures of habit and have daily work routines based on where they enter a building, what elevator they use, the location of their office or desk. Over time, employees establish their work patterns and the analytics system learns what doors they enter and exit and when they move about. It understands

their behavior.

The analytics system applies a risk score based on people, location and time. The score is higher for a person who has access to critical areas such as the data center. A location score would be higher on a data center card reader than a cafeteria door, and scores are lower during the workday and higher during off times.

By understanding an employee's habits and applying scores to the readers throughout a facility, an overall risk score is established for each employee. Baseline scores demonstrate normal behavior. However, if an employee tries to enter a bank in the middle of the night, the behavior would raise the score.

When a person's risk score rises above normal, an alert in the dashboard notifies the security team. They can then review the specific employee's behavior and see if the suspicious behavior is an anomaly or requires further action. Maybe the employee was working late on a project and needed to get into another department that he didn't have access to after-hours. Or maybe the employee is searching for account data to sell.

An analytics system flags possible early warning signs and alerts the security team to keep a better watch on the situation. Having insight early could prevent a possible breach or crisis because the security team can start to watch the behavior more closely. It will also provide HR teams and management just-cause to investigate and confront the employee about the suspicious activity.

Obtaining this level of insight from your access data is only possible using an analytics system.

adriaticfoto/Shutterstock.com

"Most banks have deployed an access control system to manage access throughout their complicated environment."

LEAST PRIVILEGED ACCESS HELPS MEET COMPLIANCE

When employees start a job, they are given an access card. Often that access card allows them access to many more areas than they need to perform their job, creating a risk. Tightly controlling employee access helps prevent risk. Using an identity management system, banks must implement the least privileged access approach, which gives employees access to only the areas they need to perform their jobs.

Access to additional areas must be requested by the employee. Access is granted for a predetermined amount of time and automatically deactivates access when the time limit expires. It provides an electronic log of all requests and an audit trail to prove compliance. Least Privileged Access works well in heavily regulated industries such as banking. Financial institutions can match up timeframes with regulations to meet compliance.

Each department within a bank works with different files and uses its own standards to complete work. Based on the security program's rules, the security team should know exactly who within the department should have access to the files, who outside the department is accessing those files, and monitor who tries to get access to those files.

"Banks must monitor all card swipes in areas where physical account data resides," said Dan Bissmeyer, G4S director of business development. "Anyone from outside that section of the building or another department could possibly be fishing for that data."

COVID-19 CHALLENGES

The onset of COVID-19 earlier this year brought on new challenges for financial institutions. Banks found themselves scrambling to move employees home to work. Entire security operations centers and call-centers needed to operate from home. Although considered essential, headquarter operations and branches operated with skeleton crews to serve customers.

Insider threat programs are set up to monitor employees, limit access, track how a person might be trying to access areas and information, and respond quickly to mitigate risk. Layers of security, using people and technology, are put in place to protect the company.

"Remote work makes it incredibly difficult to keep an eye on people," Bissmeyer said. "You lose what you had in your layers of security with physical access, identity management and analytics."

In a remote setting, a bank must rely on its logical controls to monitor when employees log in and what they are accessing. However, the loss of physical containment is a huge challenge. When operating inside a bank, the employee is surrounded by layers of security that are put in place to protect them and the data they manage. When working remotely, an employee can work anywhere, exposing data on an open laptop to roommates or friends. Printing at home is especially dangerous. Financial hardships due to COVID-19 and the economy may also tempt employees to generate fraudulent loans.

While banks have remained open, they are slowly bringing back more employees to the workplace as restrictions are lifted. The right technology can help with the transition. An analytics system can help a bank remain in compliance and show proof that the bank is operating according to policy. If a bank is running at 50 percent capacity in their buildings, the security team can pull up a dashboard that

Cloud Programming Designed to Fit Your Life,

(and whoever you're working with these days)

DKS Cloud Programming gives you the ability to program, manage and control your DKS Entry System on any computer, tablet, or smartphone from anywhere you have an internet connection. The way the world works is changing, and so have we. Discover work freedom with Doorking's Access Solutions.

Works across all devices and operating systems.

DKS®
DOORKING®

FIND YOUR SOLUTION AT doorking.com/cloud

COVID-19 Playing Havoc in Nearly Every Vertical

By Ralph C. Jensen

Nearly every country, most business elements and certainly every person has been touched by the devastation that is the coronavirus. The banking vertical is no exception, and certainly not immune to the security challenges related to the virus.

If people aren't coming to the local bank for financial transactions, what role does security play?

Chris Sessa, director of key accounts at Salient, says his role in the security and banking world hasn't really changed that much. Other than not getting on an airplane to visit clients, it's still business as usual.

"Normally, we are involved in meetings with the customer inside their facility. COVID-19 has changed all of that," Sessa said. "We like to involve the integrator, our product reps and partner reps, but now we rely on virtual meetings to ensure our customer have what they need, and that they understand the many options available to them with our software.

"Right now, virtual calls are the way we keep customer relationships going," he said.

After an installation, Sessa said that it is his goal to make sure the customer is happy, that they like the features available to them and that he can show them more options. There is still a way to move business forward and make sure security is still front and center.

Working with the IT departments, Sessa said he also engages the security and risk management teams. COVID-19 has fostered many unwanted and fraudulent results. Certain government entities have issues financial advisories to alert banks and financial institutions be aware of secure financial risks. As is the case with any challenge, there are imposters who will try to skirt security for their own illegal gain.

"A goal of ours is to ensure we bring more innovation to the corporate bank setting, especially as we see the brick and mortar banks declining and construction of new branches slowing down," Sessa said. "Among the security details that we focus are drive through banking, and in some banks the software application of facial recognition."

Facial recognition isn't a new feature set to the financial industry as more banks and corporate settings see the solution as a benefit. Sessa said the important thing to remember is setting up the security in a way that will compliment the security role that financial organizations want to achieve.

As in many instances worldwide, there seems to be a struggle with in-person security meetings, but people are quickly figuring out what works, and while the virus is making some things difficult, people are resilient and find new ways to ensure their vertical market is safe and secure.

***Ralph C. Jensen** is the editor-in-chief at Security Today magazine.*

shows exact capacity at any moment. This ensures they are following the proper health guidelines imposed by authorities and they will meet internal and external compliance standards, which help preserve the bank's integrity and reputation.

Banks can use contact tracing tools to track employees who may have been near a person who tested positive for COVID-19. If a person tested positive or was exposed, those who have been exposed to that person could easily be identified. Visitor management systems can control and authorize visitors before they arrive. A temporary card can be used from the phone via a QR card reader, eliminating the need to touch a card. Visitors can be required to answer COVID-19 related questions and remotely sign policy documents before being allowed access to a building, ensuring compliance while keeping employees safe from exposure to the virus.

Security officers can capture events using the data from other systems to contain and recover preventing the spread of infection. Proper tracking of COVID-19 diagnoses and all events within an incident management system will help the bank remain in compliance.

CROSS COLLABORATION

Deploying the best technologies can help provide a powerful and comprehensive insider threat and security program, but to have a top-notch program, an organization must have cross-collaboration between its departments. Key stakeholders from HR, legal, IT, facilities and compliance should meet regularly with the security team.

"Reach out and discuss the benefits of having a strong relationship with different departments to not only help build an insider threat program and improve security overall, but to benefit the company as a whole," Bissmeyer said. "Eliminating silos and working cross-functionally is the only way to have a first-rate security program."

Different departments perform different investigations and cross-communication could streamline the process and benefit other programs such as workplace violence, business continuity, and crisis management. All of these programs touch other departments.

Invite members from these departments to attend regular staff meetings, and request to have someone from the security department at their meetings. Understanding what is happening in other departments eliminates surprises and helps each team be more proactive.

Together, establish workflows when incidents or crises are identified. Dynamic, distributed and auditable workflows will create a streamlined response and improve reaction time. COVID-19 challenged all aspects of the banking business. Implementing cross-collaboration communication and workflows, along with the right technologies will help banks be better prepared for the next crisis.

***Kami Dukes** is the director of business development at AMAG Technology.*

Democratizing Access

Leveraging the power of shared intelligence

By Damon Madden

Alexander Supertramp/Shutterstock.com

The COVID-19 pandemic has put financial institutions under more pressure to stay on top of fraudulent activity—as opportunists are looking for any weakness in a system that can be exploited. Moreover, as consumers turn to eCommerce and digital payments while social distancing, there's no avoiding the increased levels of associated risk for financial institutions.

As organizations prepare for more commerce to be conducted online during the pandemic, sometimes through quickly transplanted or repositioned business models, payment fraud will proliferate. In fact, research from ACI Worldwide has revealed that merchants have experienced significant increases in COVID-19 related phishing activities and friendly fraud, with non-fraud chargebacks up 25 percent in May this year. While overall fraud attempt rates fell from March (5.3%) to May (3.4%), the research shows that the average ticket price of attempted fraud increased by $18 year-over-year. This indicates that fraudsters are getting more bullish and confident in their pandemic-related methods.

For financial institutions, getting the balance right between identifying genuine payments and creating a frictionless customer experience is key. And, machine learning has emerged as an essential tool for detecting fraudulent payments among the many thousands or millions of genuine ones made every day.

THE DOUBLE-EDGED SWORD OF DIGITAL PAYMENTS

Digital payments offer many benefits including better, faster experiences for customers. However, when payments happen in real-time, the window for fraud detection is reduced to milliseconds and the likelihood of recovering fraudulent payments is far lower than with traditional methods. Essentially, as payments get faster so too does fraud — and when the money is gone, it's gone.

Further, as the volume and variety of digital payments surges so too does the volume and variety of data generated by those payments. Geo-location information, behavioral clues and biometrics provide a wealth of intelligence for financial institutions — but only if they can make sense of the deluge.

As such, machine learning plays a key role enabling financial institutions to operate at the speed and scale required to authenticate genuine payments, catch fraud as it happens, reduce the volume of false positives, and improve the time it takes to react when they do occur. With machine learning, financial institutions can flag activity that deviates from the norm but isn't necessarily suspicious. For example, when a customer logs in using a different device, it's less likely to be unauthorized access and more likely that they've upgraded their phone – nevertheless, it needs verifying.

To avoid overwhelming already

> "For financial institutions, getting the balance right between identifying genuine payments and creating a frictionless customer experience is key."

stretched staff, such as call center and support departments, and introducing more friction for the customer, these non-financial transaction scenarios — and thousands like them — need to be digitized, automated and contextualized wherever possible. This is a complex challenge, but getting it right promises to provide an additional layer of competitive differentiation for financial institutions. It opens the opportunity to provide greater fraud coverage and more seamless experiences that can be applied consistently to an organization's entire customer base, all without additional headcount in either the fraud department or service centers.

Yet to be truly effective in the fight against fraud, machine learning solutions must be agile enough to be developed, tested, deployed and updated, as either new threats emerge, or as existing ones become better understood. And access to an industry-, region- or market-wide view of possible threats – not just an internal one – is essential. It improves the decision-making performance as the "machine" interacts with more data patterns.

DEMOCRATIZING ACCESS TO MACHINE LEARNING

By enabling non-specialists to build, test and deploy machine learning models in minutes, financial institutions can democratize access to the technology. This can be done by abstracting away the complex math that lies behind these models and replacing it with intuitive interfaces that enable drag and drop model building using the 'features' of fraud as building blocks. In bringing machine learning to an organization's in-house data and in-house fraud expertise – as opposed to taking that data and expertise to a machine learning specialist – financial institutions can accelerate the time to market of fraud-fighting applications.

As financial institutions become aware of new fraud risks, additional features can easily be added to the models and the weight of evidence scoring adjusted accordingly, to ensure banks' defenses keep pace with emerging risks. This can even take place automatically, through adaptive machine learning, where the technology responds to analyst-applied 'markers' for potential fraud.

Transforming the way financial institutions use machine learning (by allowing them to adopt a business-led approach) offers greater ownership and control of their fraud detection strategy. It empowers them to act self-sufficiently without the costs, risks and time associated with the involvement of third parties in artificial intelligence implementations, and – importantly for compliance – it promotes better accountability of the solution's outcomes.

THE POWER OF SHARED INTELLIGENCE

Individual banks already have access to a wealth of data with which to develop machine learning solutions for fraud detection and prevention.

However, when that data is shared across institutions, it has the potential to create a complex and varied intelligence network that can introduce more context to every machine learning decision, exponentially increasing its effectiveness.

This 'shared intelligence' empowers unprecedented collaboration in the fight against fraud. By harnessing the power of the community to increase threat visibility and distributing enhanced detection and prevention capabilities back through the community, it creates a powerful jurisdiction- or network-level deterrent to fraud.

Shared Intelligence takes the features of machine learning models deployed by participating organizations and sends them out to a central repository in metadata format. That could be a central infrastructure (CI) or an organization to which the participating financial institutions belong (either as members or connections), where they can be tested against the community view for their effectiveness.

These features are then made available to the rest of the community for members to aggregate with their own models or to build upon as needed.

Unlike a consortium approach, which over-emphasizes its largest members' experiences of fraud, members can access the benefits of a Shared Intelligence community on their terms. The biggest contributor doesn't rule the community models and risk scoring criteria.

Thanks to its power to improve the detection of emerging threats through a scaled-up 'early-heads-up' approach to feature calculation and contribution, Shared Intelligence is set to be a game changer in the use of machine learning to fight payments fraud.

SHARED INTELLIGENCE IS SHARED COMPLIANCE

The Shared Intelligence approach has the added benefit of allowing regulators and CI owners to understand the wider fraud environment with precision, empowering them to act on new and emerging threats before clusters become endemic financial crime risks. Trends specific to organizations can be tracked and understood at any level required by a regulator, enhancing efforts to combat fraud beyond payments, such as money laundering or identity theft. Further, CI's can choose to prescribe both the contributing data and time periods to ensure data consistency across the intelligence network.

This can reduce the costs of compliance too for member organizations. First, it resolves the burden and regulatory risks for attempting to extrapolate and submit data externally. Second, if a CI mandates that organizations deploy a particular model, that model can be easily distributed and then run concurrently with their own models. Indeed, an unlimited number of models can be run and tested side by side, on live data without the risk of hindering performance. Suddenly, intelligence sharing to mitigate fraud using machine learning becomes easy with the use of a democratized method.

THE NEXT FRONTIER IN CUSTOMER CENTRICITY

Machine learning allows banks to truly build their payments risk management strategy around the customer, and not around their own channels or other organizational factors that may have little bearing on the customer's needs. It also serves to ensure that specialist resources like fraud analysts are free to focus only on the activity that's deemed the highest risk and therefore the highest priority, which machines cannot — and should not — be left to handle.

Machine learning improves the application of payments risk management frameworks and policies to boost risk mitigation (both in terms of fraud and reputational risks) and enhance compliance. It forces organizations to clearly define what their policies are, and the practical steps required to enforce them. And by removing the need for human intervention in the majority of cases, rules and procedures will rarely be bypassed since machines will always follow rules.

__Damon Madden__ is a banking cyber security expert at ACI worldwide.

Indoor and Outdoor Electrical Enclosures

You name the box, Mier has you covered!

Over 350 Standard Models

Mier PRODUCTS, INC.

Indoor/Outdoor Electrical Enclosures, Driveway Vehicle Detection & Asset Protection Systems

Welcome to Mier Products Incorporated
Enclosures, Cabinets, Boxes or Cans
Drive-Alert Detection Systems
Custom Metal Fabrication & Enclosures
Custom Paint and Screen Printing
News and Important Updates
Contact Mier & Locate Distributors

WELCOME TO MIER PRODUCTS

Metal Enclosures, Driveway Vehicle Detection & Asset Protection Systems

Specialists in Electrical Enclosures, Drive-Alert Vehicle Detection/Asset Protection Systems, and Custom Fabrication

Indoor or Outdoor

Affordable Customization

Steel, Polycarbonate or Stainless Steel

Wall-Mount, Flush-Mount, Rack-Mount or Pedestal

Many with Fans, Heaters, Air-Conditioners and Thermostats

Custom Colors, Graphic Screening, Logos, Sizes and Features Available

Mier PRODUCTS, INC.

PROUDLY MADE IN THE USA ★ FOR OVER 30 YEARS! ★

1-800-473-0213 | info@mierproducts.com | www.mierproducts.com

2020 New Product of the Year Entries

By Yvonne Marquez

We are pleased to showcase the best of the best, now in the 12th year of hosting the New Product of the Year (NPOY) awards contest. Over the years, we have seen and awarded some pretty amazing security products. This year is no different. Below, you will find multiple entries in the 2020 NPOY. Winners will be announced early this month. We appreciate the time and attention given by each entrant, and to the various staff members from each of these companies who have taken the time to put together all supporting information and images for the judges to review. This information has been compiled by our Yvonne Marquez, who has been diligently keeping all things in working order.

Company Name	Product Entered
ADT	Blue by ADT Indoor Camera
ADT	Blue by ADT Doorbell Camera
ADT	Blue by ADT Wireless Outdoor Camera
Aeroturn LLC	X-Wing Optical Glass Turnstile
Alula	Slimline Touchpad
AMAG Technology	Symmetry Business Intelligence
ASSA ABLOY (AZ)	HES 630REL Series Enclosure Lock
ASSA ABLOY (CT)	Norton 6300 Door Opener with WiFi
ASSA ABLOY (CT)	Mortise Lock Status Indicator
ASSA ABLOY (CT)	Medeco All Weather Padlock (AWP)
ASSA ABLOY (CT)	ASSA ABLOY Blast & Wind Resistant Door Assembly
Axis Communications, Inc.	AXIS Live Privacy Shield
Axis Communications, Inc.	AXIS Q9216-SLV Network Camera
Boon Edam	Speedlane Compact
Bosch Security and Safety Systems	MIC IP ultra 7100i
BriefCam	BriefCam Video Content Analytics Platform
BriefCam	BriefCam Mobile Application
CertiPath, Inc.	CertiPath TrustVisitor
Clear Skye	Clear Skye IGA
Concentric	Semantic Intelligence
Conversus Inc.	EyeDetect+
CornellCookson	EntryDefender Door
Cozaint Corp	askALICE VMS and retention solution
CubeWorks, Inc.	CubiSens AH110
CyberLock Inc	Dynamic Tags Software Enhancement Module
CyberLock Inc	CyberKey Blue 3
Dahua Technology USA Inc.	300 x 400 Hybrid Thermal ePoE Network Bullet Camera
dormakaba	Switch Tech
dormakaba	Precision 2110VI Exit Device with Intruder Function and Visual Indicators
dormakaba	DKPS Power Supply Series
Dotworkz Systems	DomeWizard
Fortem Technologies	Fortem DroneHunter F700
Gallagher	Gallagher Proximity and Contact Tracing Report

Hanwha Techwin America	Hanwha Techwin’s Wisenet TNB-9000
HID Global	HID Location Services for Digital Physical Distancing and Automated Contact Tracing
HID Global	HID Aero
HID Global	HID Signo Readers
Identiv	Identiv Body Temperature Measurement Patch
IDIS America	IDIS End-to-End Video Tech for Logistics
Infocyte	Infocyte RTS (Real Time Security)
Interface Security	Personal Protection Monitoring Service
IPVideo Corporation	HALO IOT Smart Sensor 2.0
Irisys	Irisys SafeCount Live Occupancy Monitoring Solution
Kingston Technology	KC2500 NVMe PCIe SSD
LenelS2	OnGuard Cloud Edition
LenelS2	VRx
MOBOTIX	M73 Thermal
NeuShield	NeuShield Data Sentinel
Omnilert	Omnilert App
Panasonic i-PRO Sensing Solutions	Panasonic i-PRO FacePRO
Pelco	Pelco Spectra Enhanced 7 PTZ IP Camera
Pelco	Pelco VideoXpert Enterprise
PerimeterX	PerimeterX Page Defender
Pivot3	Pivot3 Virtual Security Operations Center
PlateSmart Technologies	Powered by PlateSmart
Qumulo	P-368T High-Density, All-NVMe Platform
Radware	Radware Kubernetes WAF
Rave Mobile Safety	Rave 911 Suite with Live Stream
Razberi Technologies	Razberi Monitor - Real-time Video Surveillance Health Monitering
RedSeal	RedSeal’s Cloud-Cyber Assessment Package
Regoup Mass Notification	Regroup Mass Notification
ReliaQuest	GreyMatter
Rigaku Analytical Devices	ResQ CQL
SafeWave	SafeWave
Salient Systems	CompleteView 20/20
SALTO Systems	SALTO XS4 Locker Lock BLE
SALTO Systems	SALTO KS With PODS
Security and Safety Things	Security and Safety Things Open IoT Ecosystem
Senseon	Senseon Plus
Singlewire Software	InformaCast Command Center for Mobile
SiteOwl	SiteOwl
Speco Technologies	Speco Access with Two Factor Authentication
Verkada	Verkada AC41
VOS Systems LLC	AlertTrace
Workhorse, Inc.	WorkHorse Service Company Software

The New Heart of Security

Security Convergence and Identity become the foundation of digital transformation while COVID-19 transforms access governance

By Willem Ryan

The physical security industry has before it an incredible opportunity: to lead business digital transformation (DX) through security convergence. Make no mistake about it, this is our latest inflection point. The emergence of the cloud and as-a-service platform economy have created a sense of urgency all the way up into the corporate boardroom. DX helps enterprises become increasingly customer focused and outward facing.

A Multitude of Industries

Organizations from all walks of life across a multitude of industries —banking, financial services, manufacturing, energy and utilities, transportation, life sciences and many more have realized the importance of bringing information from the operational aspects of the company to front of the house.

Security experts now agree that the most important aspects of security start with the identity of the people accessing applications and information related to the enterprise. Are they authorized? Do their privileges extend to transactional data? How long should access be granted? Who else can see the data? Are their connections secure from attack? And how can their access be turned off when they leave the organization? What about loT devices?

At the center of converged security is people, identity and trust. And in these unprecedented times, we need to know exactly where employees were, at what time and who they were with. The changing threat landscape, now with a contagion a constant, requires a new approach relying on health and safety access intelligence—all of which comes from a common identity platform.

Extending a single digital identity that can be authenticated across logical and physical environments at the enterprise has ramifications far beyond physical security. For users, it means unified cyber-physical security, greater productivity and the ability to focus on and leverage high-value tasks rather than time-consuming manual processing traditionally associated with identity access governance.

metamorworks/Shutterstock.com

“Security experts now agree that the most important aspects of security start with the identity of the people accessing applications and information related to the enterprise.”

Instead of separate siloed departments simply coexisting and not interacting, security convergence brings together technologies from security, HR, IT and Operational Technology (OT), capturing and correlating threats and risk and addressing compliance and policy automatically. It creates a common identity across people and things, which also makes it easier and faster to engage customers and the workforce, create amazing experiences and offerings and level-up operations. It co-mingles with cyber controls, facilities technologies and even behavior analytics and risk profiles to mitigate risk holistically.

Data Says Users Want Convergence

Security convergence and digital transformation aren’t some pie-in-the-sky concepts anymore. C-Suite and facility executives who have been moving in this direction now know it’s imperative to embrace it as we respond and recover from COVID-19.

According to The State of Security Convergence in the United States, Europe and India, an ASIS Foundation Convergence Report published in fall 2019, some 35 percent of respondents said that convergence has smoothed the way to create a shared set of practices and goals across physical security, cybersecurity and business continuity teams. In 39 percent of cases, convergence has “clearly enhanced communication and cooperation.”

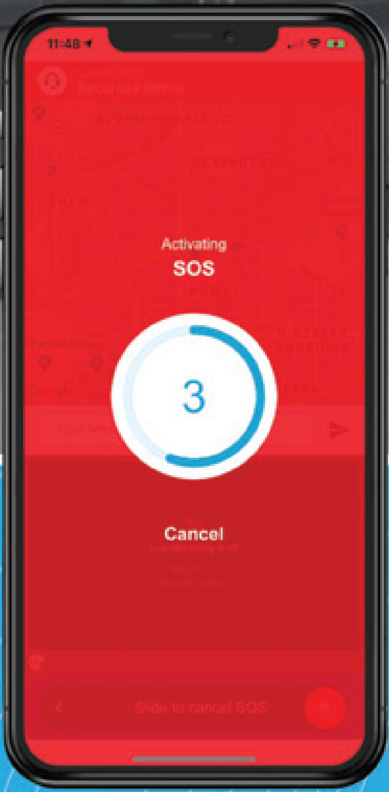
Prior to COVID-19 we also saw the following data points from the ASIS study: almost 80 percent of non-converged organizations acknowledge that convergence would strengthen their overall security function and 40 percent cited the desire to better align security strategy with corporate goals as the main catalyst for convergence. It’s likely those numbers are even higher today. Those who were already converging functions and digitally transforming probably find them-

SECURITAS
Electronic Security

- ✓ Employee-Safe
- ✓ Cost-Effective
- ✓ Compliant*
- ✓ 24/7 Monitoring

SecureStat All-Clear℠ revolutionizes openings, closings, asset-transferring and other high-risk business operations. Connected to the 24/7, UL-Certified SES Alarm Monitoring Network, rest easy knowing that in a time of threat, help is a touch of a button away.

*Bank Protection Act of 1968



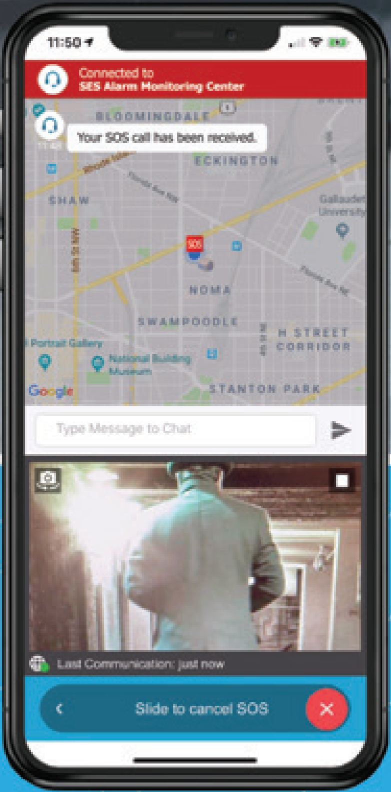
11:48

Activating
SOS

3

Cancel

Slide to cancel SOS



11:50

Connected to
SES Alarm Monitoring Center

Your SOS call has been received.

Type Message to Chat

Last Communication: just now

Slide to cancel SOS

Contact SES today to learn more
securitases.com • 1-855-331-0359

selves much more prepared to respond to the pandemic and all the new facets now part of identity management and compliance.

Businesses already down the path of digital transformation have been able to pivot, survive, thrive and serve customers and protect their workforce during these disruptive times.

Enterprise security leaders now understand that the effects of a cyber breach, physical attack, manufacturing loss, or contagion on site far outweigh the costs of a holistic and converged system. Those who embrace the digital transformation will enable cohesiveness of systems and data, with the end result delivering proactive threat detection and prevention— a unified threat response to mitigate risk and greater situational awareness.

Identity Management With Muscles

Identity management software platforms integrate with HR programs and processes to bring together the human side of security, working in tandem to create a better and safer enterprise. Identity management with Identity Intelligence technology that incorporates artificial intelligence and machine learning can set risk scores, adding filters and exceptions to flag, escalate and detect anomalies in access and even production processes. Active policy enforcement rules-based engines automatically identify policy violations and unauthorized access as well as operational and procedural issues. In addition, identification credentials automatically expire and are taken offline when access is no longer granted, reducing risk from a disgruntled employee in-house.

The power of security convergence is most evident when it automates and detects seamlessly across more than one domain, like IT and physical security. Consider this real-world scenario: a utilities company employee enters the company through the main lobby, takes the elevator to his floor and badges in to gain access through that level's main door. He proceeds to his desk and signs into the company network to access his email. At the same time someone is using the identical access credentials remotely via the VPN. Obviously he can't be physically present locally and remotely.

A converged platform detects the external intrusion by automatically identifying the access anomaly and allows security to immediately disable access, preventing a potential threat.

Now, let's put this in a COVID-19 context. With the pandemic and the return to work, modification to identity management is required for safety, company policy and compliance reporting. Workforce

Health and Safety access governance software solutions help organizations open safely in a frictionless, controlled and secure way by automating and enforcing COVID-19 related policies and procedures. Automated batch email/text notifications with self-service links send requests to the remote workforce for self-attestation and self-reporting offsite and enable access by the worker to the facility based on health, travel and other company policies. Physical security can help enforce health and safety policies through technology, including reminders, prompts, automation, self-attestation and more.

Here's an example: An employee completes the self-reporting health and travel questionnaire, which triggers workflow based on answers. These health questionnaires collect data and document employee activity during lockdown, including infection, symptoms or exposure. The request routes to the manager for action and the workflow can be configured to specific needs.

Once the manager reviews the request, it is determined that based on the answers the employee is high risk and per policy his access will be revoked for 14 days while in quarantine. Enterprises administer the self-service process to view, edit and approve health exposure risks of the workforce and disable access based on policy.

When the quarantine period is over, the employee receives an automated notification to request reinstatement and the self-attestation questionnaire. The employee is cleared and requests to be reinstated, following work flows to provide supporting documentation, such as a medical discharge or physician's letter. Access is reenabled and the employee is notified with instructions to come to work.

Health and Safety access governance and intelligence provides support for prescreening of the workforce during site entry with automated policy enforcements. Pre-registered and onsite visitors/contractors check-in/check-out with prescreening, watch list and other checks prior to access. In the production or distribution facility, Health and Safety analytics track confirmed or potentially exposed COVID-19 workers, identify exposed areas for lockdown and/or sanitization, social distancing violation, location heat map and other actionable health and safety analytics.

Identity management also allows you to automate your communications and deliver clear expectations and procedures to your workforce, visitors and contractors pre-visit and onsite— adding to a seamless experience.

Real-time Active Enforcement

Technology like Identity Intelligence and the active policy enforcement rules-based engine automatically identify policy violations and unauthorized access. This allows security managers to proactively monitor and respond to security violations as well as operational and procedural issues. During the COVID-19 outbreak, this could include travel history to restricted countries or regions. Integration with travel and HR applications can detect when and where a person booked travel and has badged in, providing the enterprise the ability to build a solid risk profile of activity. If someone in the workforce recently visited a restricted location, security and HR teams can be automatically notified to disable badge access to help avoid exposure and potential transmission. In the scenario where someone in the workforce becomes sick they would be considered a high risk. Any requests for physical access to a facility would require special approval according to company and local or federal health authority policies.

With an outbreak, modification to the visitor experience is also required. It is the first point of contact and along with lobby and security staff is part of the front lines for safety. Enterprises can configure their Visitor Identity Management (VIM) system to provide clear communication of current policies during the outbreak, reinforcing WHO best practices. VIM can easily be configured to prompt guests to answer specific screening questions related to recent travel and sign off on legal documents.

Security is no longer simply about keeping bad guys out. Security has become the business enabler during the digital transformation. It's now the fundamental component of protecting people and workspaces and identity stands at the center.

__Willem Ryan__ is the vice president of marketing and communications at AlertEnterprise Inc.

Why Lone Workers are Vulnerable

What any business can do to protect staff from life threats at work

By Brent Duncan

The economic slowdown created by the pandemic has forced many retail chains, restaurants, hotels, banks and financial institutions with a retail presence to cut back on staff and change their business models.

Curbside Delivery

For example, many retail chains have started offering curbside delivery that forces employees to step out of the stores. They have also cut back staffing levels resulting in situations where a single employee is left to manage the third shift or handle store closing or opening at odd hours with no backup or a co-worker around. While lone employees play a critical role in keeping the business up and running, they are more at risk of encountering life threats at work. As COVID-19 and social strife continue to wreak havoc, businesses are actively evaluating options to secure and monitor the safety of their lone workers so they can work with confidence.

Lone workers have always been an important part of certain industries and businesses. Historically, convenience stores have always employed solitary workers during the third shift. There are few sales going on overnight, yet it's still a 24-hour business.

Whether it's taking the garbage out, delivering merchandise to customers outside the premises, or making a run to the bank Now, more than ever, employees in retail chains are finding themselves working alone. Retailers have to now proactively roll out security solutions that will give their lone workers an option to seek help if they feel threatened.

Likewise, hotel cleaning staff and maintenance crews typically work alone even when occupancy is high. Recently, hotel chains that are members of the American Hotel and Lodging Association have chosen to proactively implement a safety program for all hotel personnel.

The program includes a mandate to provide all staff with safety devices with the objective of preventing or responding to sexual harassment and assault. The 2019 Hotel and Casino Employee Safety Act (S.B.75) in Illinois mandates a personal protection device for all employees working alone. New Jersey, Washington and California have already enacted similar laws requiring hotels to provide their employees with a wearable panic button/safety device.

Banks are also looking for ways to protect employees as they too want the option to open with just one employee without the presence of an armed guard. They want to ensure the safety of employees who leave the inner perimeter of the building such as when servicing remote ATMs.

Mitigating Risk for Lone Workers

For many businesses struggling to stay afloat, employing a full-time security guard is not sustainable and loss prevention experts know that guards carry their own risks because you now have an authority figure on site and maybe even a firearm involved.

There have been instances when a guard's firearm caused an issue at a location. At the same time, relying solely on a video security system when action and intervention are required may not always be a viable solution.

The ultimate goal is to minimize lone worker risk and ensure employee morale and well-being. The solution has to be simple and robust enough that employees want to use it. It should require no installation, and no configuring by the end-user. It needs to be small, lightweight and unobtrusive until it is needed.

Lone Worker Monitoring Solutions

To address these challenges, there is a new breed of smart, wearable, and discreet personal protection devices on the market. These devices enable businesses to add another layer of protection for their associates when they are working alone. Wearable personal protection devices can be worn on a lanyard, belt, vest, jacket or pants and provide a cost-effective option for retailers and businesses who want to give their lone workers the protection they deserve.

Phone-based apps can also serve the purpose. However, they fall short as they require several steps to turn on, launch and use, and may interfere with phone calls and other device functions. Visibly fumbling with a personal cell phone can also cause certain situations to escalate prematurely If an assailant suspects the victim is calling for help or backup.

Personal safety monitoring devices have one major advantage. They are always-on, come with a single-push panic button that silently dispatches police and connects to a live monitoring service in just a few seconds.

A properly designed personal protection device delivers

It takes a Viking to...

DEFEND YOUR CASTLE.

Let's face it, part-time security isn't good enough. You need it **24/7**. Day in and day out. Year after year. **You can't afford to mess around with wimpy security.**

That's why our rugged entry system and access control gear has been **battle-tested** to withstand the harshest elements and toughest intruders.

Our innovative designs, tough-as-nails craftsmanship, expansive product line, and best in class customer support have secured Viking's role as a **leader** in the security and communication industry for over 50 years.

YOU NEED A VIKING.

SECURE YOUR BUILDING FROM INTRUDERS.

VIKING

715.386.8861
VIKINGELECTRONICS.COM

USA | DESIGNED MANUFACTURED & SUPPORTED

> "As COVID-19 and social strife continue to wreak havoc, businesses are actively evaluating options to secure and monitor the safety of their lone workers so they can work with confidence."

comprehensive situational awareness by sending time and location stamped GPS coordinates to authorities. It also opens a two-way audio communication channel with the employee and captures evidentiary grade photos to provide hard evidence for law enforcement. Because the units are cellular-based, there's no limit to how far an employee can be from the business which means that it is perfect for curbside delivery and even home delivery use cases.

When the panic button is pressed, how the emergency is handled is just as important as the device itself. These personal protection devices can work in conjunction with a fully interactive video and two-way audio security system. When combined with a rapid-response 24/7 central command center staffed with security professionals, it becomes the most comprehensive and cost-effective life-safety and asset protection system on the market.

An interactive monitoring solution further augments a personal protection device by offering remote security escorts, remote tours, video verified alarms, and even operations compliance services to organizations. With more camera eyes and ears on the ground, the opportunity to de-escalate situations further increases and deters employee shrink as well.

Keeping Lone Workers Company

Lone workers don't have to be completely alone. Having an experienced security professional and law enforcement available at the touch of a button can boost morale and give lone workers the confidence to do their jobs without taking on unnecessary risk. Interface Security Systems recently launched a wearable personal protection monitoring solution in partnership with Risk-Band. This new service is directly integrated with our interactive 24/7 Central Command Centers. A single push of a button provides two-way voice communications, user profile data, near real-time images, and geolocation data to Interface's trained security professionals who can immediately assess the situation, intervene and deploy the appropriate emergency response.

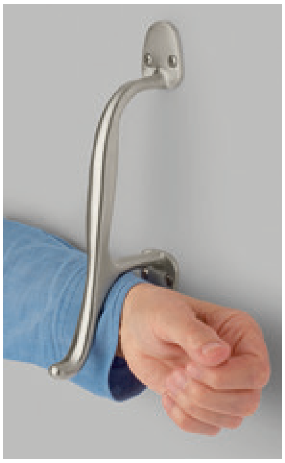
In a time when more attention needs to be placed on protecting assets and increasing safety measures for employees and customers, this new service enables businesses to make wearable safety devices an essential component of their emergency response strategy.

__Brent Duncan__ is the chief revenue officer at Interface Security Systems.

SECURITY today
How The Restaurant Industry Is Handling Renewed Active Shooter Threats
...for NEMA TYPE 4X Enclosures
Most Popular Articles

ASSA ABLOY
Opening Solutions

Experience a safer
and more open world



Just Hook *an* ARM, or Pull *with a* FOOT

Reduce of skin-to-surface touchpoints with Rockwood arm and foot pulls. These simple, low-cost additions provide hands-free door operation for new and pre-existing aluminum, metal, or wood openings.

Rockwood Hands-Free Door Pulls are part of a continuum of Safer2Open™ low-touch and touchless door hardware solutions from ASSA ABLOY.

Visit assaabloydooraccessories.us, assaabloydss.com, or call 1-800-458-2424 to learn more.

How to Prepare Your System

COVID-19 exposes threats and vulnerabilities as companies reopen

By Rich Mellot

The impact of the COVID-19 pandemic has challenged companies' security in new ways and exposed an increasing number of threats and vulnerabilities. As they plan to reopen and consider their company's future, security teams will not only need to evaluate their current security systems but better understand what security means to them in the new norm.

Managing people on your company's property through access control systems will matter more than ever before. While you likely added or changed your company policies regarding access during the pandemic, it's time to consider how you'll prepare for the post-pandemic mindset. This means security teams will place greater value on the ability to track and manage traffic flow and understand exactly who is coming and going from their facility.

In addition, to ensure that all individuals in and out of their facility have been properly screened at the point of entry, some businesses are even talking about post-entry screening as changes can occur throughout the workday.

Looking ahead, there are essential tools and resources you'll need to prepare for the post-pandemic working world.

ENHANCE YOUR VISITOR MANAGEMENT SYSTEM

With employees and visitors returning to offices, companies want to more effectively screen those who are accessing their premises. Visitor management systems have been used before to screen and grant access to on-site visitors, but those systems are maturing. Some now include contractor, vendor and employee identity management, pre-screening questions, hygienic touchless interfaces and tools to automate workflows and ensure proper compliance with company policies.

Because of these improvements, advanced visitor management technologies can provide an important security layer to your access control policies, enforcing compliance and integrating seamlessly with your current security systems.

For example, human temperature screening devices, which scan exposed skin with thermal imaging sensors to detect elevated temperatures, can add an extra screening layer to your visitor management system. Some of these systems deployed require staff to monitor the screening process, while others include additional automation to allow for more flexibility with the overall solution.

These systems, however, still require periodic monitoring to ensure the environment or other conditions do not impact the accuracy of your subject's skin temperature readings. Depending on the solution, day or time of year, it may require adjustments for temperature deviation, thresholds or recalibration.

Also, depending on your company's location, you may be governed by specific regulations like EEOC, ADA, HIPAA and FDA compliance requirements, so ensure your system meets those expectations and that your internal policies reflect them.

> "While you likely added or changed your company policies regarding access during the pandemic, it's time to consider how you'll prepare for the post-pandemic mindset."

A major misconception around human temperature screening technology is that it can detect viruses like COVID-19. These solutions cannot detect surface contamination nor asymptomatic individuals, and higher skin temperature does not always equate to illness. Ensure you follow CDC guidelines and be aware of your state and local requirements. These screening devices are part of your larger access control system and strategy. They're tools that are part of a policy and program to help you mitigate risk of your visitors and human assets.

Another area of risk in these systems is the pen and paper logbook: manually tracking visitors to your property is time-consuming and difficult to use to enforce policies, not to mention creating a common touchpoint where illness could be spread. Instead of paper, electronic visitor management kiosks let companies easily screen and track people, and produce visitor badges without manual management from additional company staff. You can also ask screening questions at the digital kiosk, such as recent travel locations, health symptoms or exposure to others who were diagnosed with COVID-19. The benefits of kiosks extend to as many sites as you have, with increased convenience, compliance and visibility across your company.

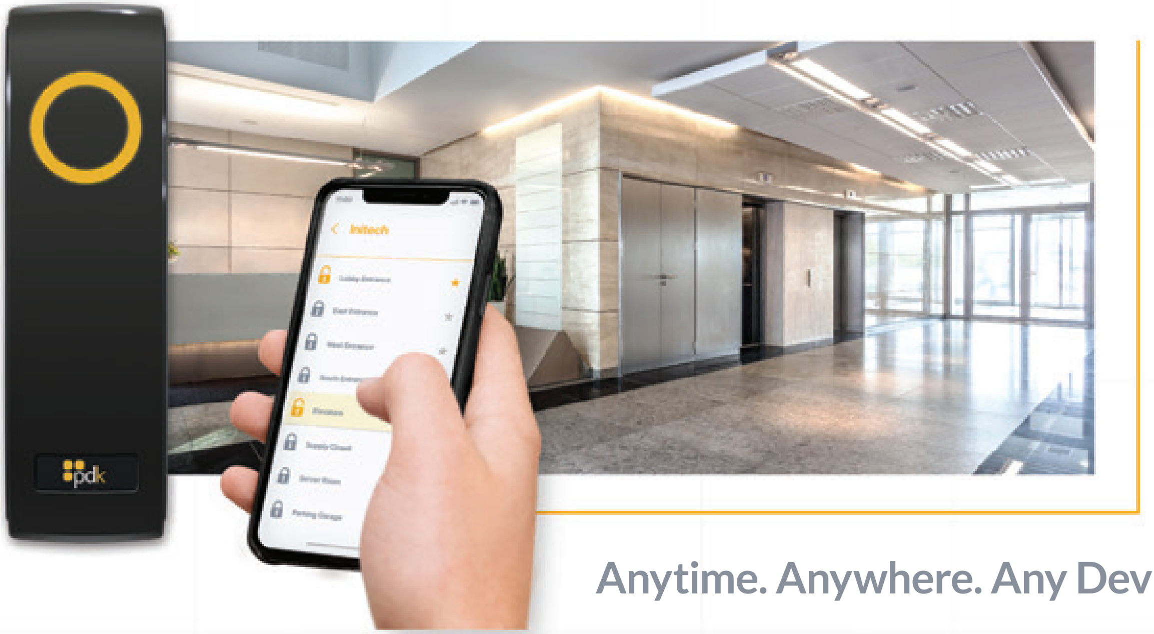
IMPLEMENT CLOUD-BASED ACCESS CONTROL SOLUTIONS

When companies closed offices and moved teams to remote work, it showed many security teams the importance of being able to fully access their systems for remote management to adapt quickly and respond to the new security environment, needs and potential threats. While your on-site access control may have included steps like checking exterior doors, collecting master keys and conducting access audits, moving to a remote setting requires new cloud-based technologies to give you a more omnipresence within your business to respond to threats with deeper levels of operational insights.

As we've seen during the pandemic, many companies needed to update their access privileges quickly with limited staff access to pdk™

mobile-first accesscontrol

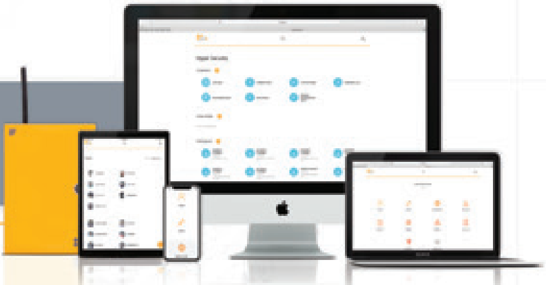
Your phone is your key



Anytime. Anywhere. Any Device.

The only-true 100% mobile-first access control solution
for employees, tenants, administrators, and installers

- Complete installation & management from the mobile-app
- Remotely unlock your doors with the push of a button
- Use your phone as an encrypted access credential
- Keep your phone in your pocket for hassle-free entry



801.317.8802
prodatakey.com

their locations. Processes like adding or revoking user access credentials remotely can be accomplished more effectively with cloud-based access control. Beyond granting privileges, these systems can also enable mobile credentialing as an easy-to-manage contactless solution to reduce viral spread and increase efficiencies. Stored in users' phones, mobile credentials can be integrated with fingerprint and facial recognition capabilities to increase security.

Coupled with other cloud-based solutions like video surveillance as a service and intelligent service assurance monitoring, your access control system can monitor and protect your property, ensure access is granted to the right people, operational uptime and performance monitoring and allow your team to control everything from anywhere and at any time. You can reinforce your security policies, including whatever changes you've made since the pandemic began, to protect your employees and assets.

PROTECT YOUR PREMISES WITH ALARM VERIFICATION

The pandemic has left many communities strained with public resources like police officers and other emergency responders. In efforts to limit human contact, some cities have chosen to limit in-person responses to certain calls like breaking-and-entering reports without suspects or the potential to recover lost property. Companies may have the right security components in place, however, they also must ensure their security system can verify when a situation is occurring and notify the right people in time.

Alarm verification systems use video and audio technology to enhance the monitoring of your premises when an alarm is triggered. A monitoring center operator can then confirm a human presence – rather than a false alarm triggered by a stray animal or an HVAC system kicking on, for example – and assess the threat level to your company. These systems provide actionable intelligence that a crime is being committed and capture the details police will need to apprehend the intruder.

Use of advanced alarm verification technology reduces false alarms, thus leveraging police resources for known alarm events and potentially increasing your call priority, which can lead to more apprehensions. Alarm verification vendors have seen that police respond up to 85% faster to verified alarms as opposed to unverified ones, and for one vendor it has led to over 180,000 documented apprehensions – many before entry was made. If your company wants to add more power to your intrusion detection system and avoid costly false alarm fees, consider alarm verification.

SECURE YOUR NETWORK WITH CYBERSECURITY TOOLS

When the workforce shifted primarily to remote officing and business owners/leaders closed access their facilities due to COVID-19, the shift in work brought additional cybersecurity threats to the table. In April 2020, a few weeks after stay-at-home mandates began, the FBI's Cyber Division reported up to a four-fold increase in daily cyber attack reports. As companies adopt more network-based solutions and add more components to their security systems, cyber attacks can be expected to continue rising.

Adequately protecting new systems is proving difficult for many companies since they struggle recruiting and retaining the right talent. Information Systems Security Association (ISSA) and industry analyst firm Enterprise Strategy Group (ESG) found that almost three-quarters of organizations are affected by a lack of available cybersecurity talent. There's a dearth of the needed skills in the marketplace and a lack of resources on the company's side to retain dedicated cybersecurity staff. Yet, enterprise networks are becoming more complicated than ever before, and with the introduction of cloud-based tools and environments, cybersecurity is an even more critical need.

In response, companies are turning to technology and professional services to help mitigate cybersecurity risks to their environment. Network protection solutions can keep a company's network, devices and data safe from attacks like intrusions, malware, ransomware, phishing and malicious files. These solutions can also protect remotely connected IoT and other IP-connected devices, which are being exploited more as a result of the pandemic shifting workforces away from the office. Coverage with the proper cybersecurity tools and supplemental services can prevent future financial disasters and ensure your network stays fully functional.

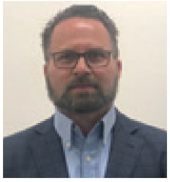
ADD REMOTE SERVICES TO YOUR PROFILE

Even before the COVID-19 pandemic, remote security solutions were a growing trend. But with more strain on company personnel and budgets and increased restrictions for on-site visitors, security teams will rely more on remote security management than ever before. While your security team may have implemented specific remote services to fill in gaps during the pandemic, the future will require a more comprehensive solution that addresses security needs befitting updated company policies and the new norm.

Remote systems for on-premises use include several options for monitoring. After you've installed security cameras applied to your specific application needs, a monitoring center operator can conduct remote "guard tours," visually surveilling the property on-demand or based on a schedule to look for potential threats or intruders. Some systems even allow guards to speak through the camera to anyone on-site, or for the system to play a pre-recorded message when an analytic detects a person breaching the property or perimeter. When compared to an on-site patrol, this system can save you up to 80 percent of your personnel cost.

Beyond monitoring, remote services can include round-the-clock site management. A monitoring center can manage person or vehicle access to the building, conduct video surveillance and speak through intercoms, taking over or supplementing responsibilities carried out by on-site staff. A service provider may also offer an online portal for you to manage the services you're using, view reports and handle issues like service calls and billing. Even when your staff can't be on-site, remote services can help you protect access to your property and assets.

While the pandemic has brought to light many new challenges and threats to security, you can rely on your security systems to mitigate threats to your premises, assets and people. The addition of technologies like human temperature screening devices, cloud-based access control and video, automated service assurance and remote managed and monitored services can ensure your security solutions have the ability to respond to the immediate challenges created by this new norm and the ability to plan ahead for the ever-changing challenges that come within your security landscape.



__Rich Mellott__ is a director of Technology & Product Management at STANLEY Security.

Kingston TECHNOLOGY

Uncompromising Data Security

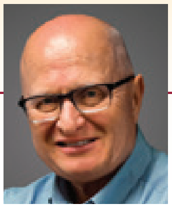
AES 256 ENCRYPTION · FIPS Level 3 Certified 140-2 · TAA COMPLIANT · SECURITY today GOVIES

KINGSTON ENCRYPTED USB DRIVES

www.kingston.com/us

SECURITY TODAY SOLUTIONS

Compiled by Ralph C. Jensen, Editor-in-Chief



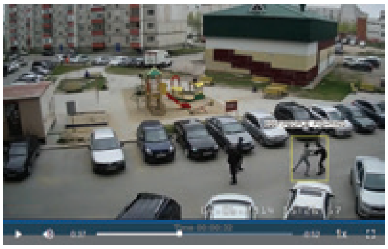
Paxton
Net2 v6.04
Occupancy Management
Control and monitor social distancing with Net2 Occupancy Management
Main Office Building
88%

Net2 Occupancy Management

Paxton has brought new additions to its leading Net2 access control product line, helping installers make their customers' buildings more COVID-secure. The latest version of Net2 – v6.04, has been in rapid development since May and is now ready for installers to download. It features Net2 Occupancy Management which allows you to limit the number of people in any given area; either barring access or sending an email or text to the building manager when a space nears capacity. It works across multiple areas of a site and can be set to operate a one in, one out system to support social distancing measures. In addition to this update, installers who want to use thermal scanning to help limit the spread of the virus can do so with three new thermal scan integrations.

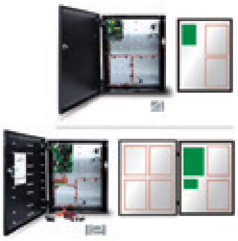
Powerful Encoding Capabilities

SALTO Systems has released the NCoder – a contactless smart card for next-generation access control systems that integrates the encoding capabilities of a powerful updated design encoder with a built-in desktop reader function. The SALTO NCoder configures permissions and user access plans for user credentials or hospitality guests. It is compatible with a wide range of RFID cards and mobile keys. SALTO SPACE data-on-card-platform system operators – by defining their own user access plan and building properties with ProAccess SPACE web-based software – can rightfully take control over user rights management of their building access system. Security meets design with the SALTO BLUEnet generation of smart locking access control products and the NCoder is no exception.



Changing Landscape in Video Intelligence

viisights, Inc., the developer of innovative behavioral understanding systems for real-time video intelligence, continues to gain momentum with cities, organizations, and technology partners serving the U.S. market. The highly innovative and unique solution provides municipalities and organizations with the ability to automatically detect, analyze and differentiate human behaviors, such as an individual slipping and falling vs. being thrown to the ground, or two people embracing vs. fighting, or a peaceful parade vs. a riot. viisights' powerful solution also delivers analytics ideal for helping organizations get back to work safely.



Streamlined Single-voltage Pre-wired Solutions

ProWire Unified Power Systems has expanded its family of products with the introduction of ProWire XPRESS, a new value line of single-voltage power systems featuring prewired controller terminal strips for rapid, reliable setup and in-the-field savings. ProWire XPRESS models come prewired for system power, faults, communication and tamper switch. Models are currently available for Mercury Security controllers in four-door (FPV4-E2M/T4X) or 12-door (FPV102-D8PE2M1/T12X; FPV104-D8PE2M1/T12X) configurations at 12 or 24VDC. ProWire XPRESS carries a joint Mercury/LSP UL, ULC certification and CE listing (EU).

Device Achieves 3-hour Rating

Securitech Group is pleased to announce that SAFEBOLT™, the award-winning red button locking solution, has increased its fire rating for up to three hours. SAFEBOLT™ is the first barricade lock that respects all fire and life-safety codes for safe-haven locations such as classrooms, offices, houses of worship and other spaces. SAFEBOLT™ empowers anyone in the room to safely secure the door without dangerously trapping others. Designed in full compliance with existing NFPA, IBC (International Building Code) and other codes, AHJs (Authorities Having Jurisdictions) do not need to write exemptions to allow the use of SAFEBOLT™. Simply pressing the red button projects a 1" stainless steel locking bolt to secure the room.

Temperature Scanning Solution

Johnson Controls announced the launch of its smart elevated skin temperature scanning solution, the Tyco Illustra Pro Thermal EST. A healthy and safe environment starts with a holistic approach that encompasses not only a building's heating, ventilation, and air conditioning infrastructure, but adds temperature screening among protocols including contact tracing, frictionless entry and exits, and the practice of social distancing. This contactless and highly accurate solution will be another tool in the first line of defense for building owners and operators as part of their pandemic safety measures. The Tyco Illustra Pro Thermal EST camera provides rapid scanning at accuracy levels that exceed standards set by the International Electrotechnical Commission (IEC), as tested and confirmed by Underwriters Laboratories (UL).

LIFE IS DIFFERENT TODAY
How will your workplace respond?

Drone Detection Device

DroneShield Ltd is pleased to announce the upcoming 2Q2020 software release of its RF-based threat detector for its various counterdrone products, including body-worn RfPatrol MKIITM platform. The software upgrade will be available for all customers and fielded devices starting July 1. RfPatrol MKIITM is a body-worn passive (non-emitting) drone detection device. As the drone threat rapidly evolves, DroneShield provides quarterly updates to ensure its customers receive continuous counterdrone protection. 2Q2020 quarter update includes a number of new drone models from multiple manufacturers, as well as performance enhancements and general firmware updates.

Making Access Management Simple

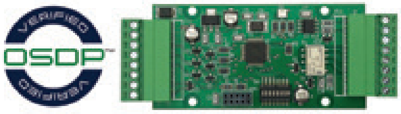
Bosch Building Technologies is introducing its Access Management System 3.0 as a simple, scalable and always available solution. Today's market wants access control systems that are always available, scalable, and integrated with other security solutions like video and intrusion systems to ensure the highest security and safety levels. At the same time, these systems must be easy to configure and use. With the introduction of the Access Management System 3.0, Bosch meets all of these requirements. The system is designed to be available at all times. Its resilient design includes a Master Access Controller (MAC) as an additional layer of defense between the server and the access controllers.

Antimicrobial Security Tray Technology

Leidos is upgrading the Edinburgn Airport Limited security tray returns with its antimicrobial tray technology. The technology will minimize the spread of bacteria in an airport setting from person to surface contact. The security trays prevent reproduction of a broad spectrum of bacteria, including staphylococcus aureus (staph), E. coli, and antibiotic-resistant bacteria like MRSA and VRE, by 99.99 percent. The antimicrobial technology is built into the security tray during Leidos' tray manufacturing process and continuously minimizes the presence of microbes throughout the security tray's lifecycle.

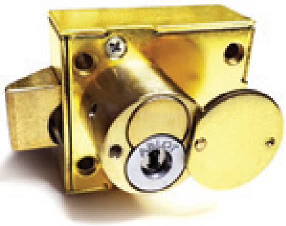
Long-term Video Retention

Cozaint Corporation, has announced the launch of askALICE, the industry's most economical video surveillance management hardware and software system delivering extreme long-term retention. askALICE provides an enterprise-grade video management software suite integrated with server and multi-tiered storage. Cozaint has developed the capabilities of the VMS software to easily play back video from either initial storage or second-tier storage without any additional steps needed by the surveillance operator. This breakthrough now enables the Cozaint VMS Software —named BOBBYvms— to seamlessly and effortlessly play video from various tiers of storage.



Converter Attains Certification

The Cypress OSDP-Wiegand Converter has attained certification by the Security Industry Association's OSDP Verified program. The OSDP Verified mark validates that a device conforms to the SIA Open Supervised Device Protocol (OSDP) standard and its related performance profiles. One of the first devices to receive the OSDP Verified designation, the Cypress OSM-1000 Converter is a sought-after solution for adopting OSDP, which became an international IEC standard this year. OSM-1000 offers a choice of 2 operating modes. When used in PD (Peripheral Device) mode, it connects a traditional Wiegand reader to an OSDP access control unit. When used in ACU (Access Control Unit) mode, the OSM-1000 connects an OSDP reader with a legacy Wiegand access controller.



A unique Traffic Enclosure Lock

ABLOY USA is the first company in the United States to offer a uni-versal hybrid mechanical/electromechanical product with the introduction of its new Traffic Enclo-sure Locks. The 75481 series provides several key access control options using less cylinder and offering greater accountability. The 75481 series provides the right solution for three distinct applications. The first is product specific with less cylinder, such as any Key-In-Knob Schlage. There also is the mechanical PRO-TEC2 and the electromechanical ABLOY CLIQ™. The need to secure traffic critical infrastructure is becoming more complicated due to new traffic cabinet technology.

AD INDEX

FREE PRODUCT INFO

Quick, Easy and Direct...get the info you need NOW!

Go online to www.securitytoday.com/productinfo to request free information from advertisers in this issue.

ADVERTISERS

Info No.	Company Name	Page
	ADT Commercial Security	55
	Alula	19
	Altronix	3
	Allied Universal	31
	ASSA ABLOY EMS/ESH	21
	ASSA ABLOY EMS/ADAMS RITE	37
	Assa Abloy DSS	49
	Axis Communications, Inc	59
	Boon Edam	9
	Camden Door Controls	29
	CyberLock, Inc.	15
	Delta Scientific	7
	Door King	33
	Dotworkz	27
	Garrett Metal Detectors	17

Info No.	Company Name	Page
	IP Video Corporation	35
	Kingston	53
	MIER PRODUCTS INC	39
	NIGHTLOCK	2
	Panasonic Corporation of North America	60
	ProdataKey, Inc.	51
	Safety Technology Int'l, Inc	45
	Sage Integration	25
	Salient Systems Corporation	5
	Securitas Electronics Security, Inc.	43
	Security Today Academy	18
	Security Today	28
	Security Today	48
	THE HOUSING COMPANY	11
	Viking Electronics	47
	Winsted Corp.	23

Security Today Solutions

Info No.	Company Name	Page
	ABLOY USA	56
	Bosch Building Technologies	56
	Cozaint Corporation	56
	Cypress	56
	DroneShield Ltd.	56
	Johnson Controls	54
	Leidos	56
	Paxton	54
	ProWire Unified Power Systems	54
	SALTO Systems	54
	Securitech Group	54
	viisights inc	54

Reprints: For single article reprints (in minimum quantities of 250-500), e-prints, plaques and posters contact: **PARS International**
(212) 221-9595
1105reprints@parsintl.com
www.1105Reprints.com

List Rentals: This publication's subscriber list, as well as other lists from 1105 Media, Inc., is available for rental. For more information, please contact our list manager, **Jane Long**, Merit Direct. (913) 685-1301; *jlong@meritdirect.com*; *www.meritdirect.com/1105*

Media Kits: Direct your Media Kit requests to **Lynda Brown**, (972) 687-6710 (phone), (972) 687-6750 (fax), *lbrown@1105media.com*

INDUSTRY PROFESSIONAL

With Randy Smith

Controlling the Cogeneration Plant for Hudson Yards

Towering over the Hudson River on Manhattan's New West Side is Hudson Yards – a cultural epicenter with more than 100 diverse shops, residences and culinary experiences. By area, it's the largest private real estate development in the United States – covering more than 18 million square feet over seven city blocks.

Early in the planning process, the Hudson Yards development recognized the opportunity to power Hudson Yards in a resilient, effective and sustainable way. The answer was a 13.3-MW cogeneration (CoGen) plant.

"The plant is a green initiative, we wanted to limit the greenhouse gasses by burning natural gas onsite, said Nick Lanzillotto, vice president of MEP-HRY Development. "It means we use about 80 percent of the energy the plant produces both electrical and thermal energies, as opposed to around 30 percent of the energy from commercial electric suppliers."

NOT YOUR TYPICAL POWER PLANT

The CoGen plant at Hudson Yards serves all the buildings in the Eastern Railyards development. The buildings energy needs are met with Cogen as well as the buildings own infrastructure. It's a complex system that requires a master control room to keep everything operating smoothly.

"We needed to set up a control center that's more typical of a power plant and a district energy plant rather than a typical New York City skyscraper," Lanzillotto said.

Nick had a vision for this control center. Well into the center's development, he realized his vision wasn't being achieved. That's when he discovered Winsted.

"I happened to visit Winsted website and saw images of control room layouts, they just had the right feel," Lanzillotto said. "That's when we brought Winsted into the project."

Anton Gvozdikov/Shutterstock.com

A SEAMLESS PROCESS – FROM CONCEPT TO INSTALLATION

From concept to installation, the setup was smooth and seamless. So much so, that Lanzillotto wished other Hudson Yards projects would follow suit.

"If the whole project went as easy our work with Winsted, it would've been great," Lanzillotto said. "The Winsted team was wonderful to work with. From rendering to layout, to determining the right components, all the way to installation, it all went very smooth.

In total, the CoGen plant's control room contains five workstations, each with four monitors. An 8' x 16' video board stands in front of the workstations. Outside of the control room sits the information room with a single technician workstation, filing cabinets, storage cabinets and a blueprint-reading table with additional storage.

"They made it very easy for us," said Nick. "Because it was so seamless, we worked with Winstead on a fire command center that also went very well."

Randy Smith *is the president and general manager of Winston Corp.*

STAT
SPK
CONTROL
AXIS